MAS6331 / MAS6332 - Algebra 1 & 2
(Notes Only Version / With Study Material)

Jay Pantone
University of Florida

Last Edited: August 19, 2012

Contents

This packet consists mainly of notes and exercises from MAS6331/MAS6332 Algebra 1 & 2 taught during the Fall 2011 and Spring 2012 semesters at the University of Florida. The course was taught by Prof. P. Sin. The notes for the course (and consequently, these notes) follow *Algebra*, by Hungerford, though the sections covered are not in the same order. Numbering of theorems, lemmas, etc. corresponds to the numbering in Hungerford. Following the notes are the suggested and required homework assignments.

If you find any errors or you have any suggestions (including in the exercise solutions), please contact me at jay.pantone@gmail.com.

Chapter 1

Course Notes

1.1 Chapter V - Fields and Galois Theory

1.1.1 Section V.1 - Field Extensions

Definition: Let $K \subset F$ be fields. Then, F is an extension of K.

Note: We operate by starting with a fixed field K and thinking about all possible extensions F, rather than starting with a field F and thinking about all possible subfields K.

Definition: Let $u, u_1, \ldots, u_n \in F$ and $X \subseteq F$. Then,

$K[u]$ denotes the subring of F generated by K and u.
$K(u)$ denotes the subfield of F generated by K and u.

Theorem V.1.3:

$$\begin{aligned}
K[u] &= \{f(u) \mid f \in K[x]\} \\
K(u) &= \{f(u)/g(u) \mid f, g \in K[x],\ g(u) \neq 0\} \\
K[u_1, \ldots, u_n] &= \{f(u_1, \ldots, u_n) \mid f \in K[x_1, \ldots, x_n]\} \\
K(u_1, \ldots, u_n) &= \{f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) \mid f, g \in K[x_1, \ldots, x_n],\ g(u_1, \ldots, u_n) \neq 0\} \\
K[X] &= \{f(u_1, \ldots, u_n) \mid f \in K[x_1, \ldots, x_n],\ u_1, \ldots, u_n \in X,\ n \in \mathbb{N}\} \\
K(X) &= \{f(u_1, \ldots, u_n)/g(u_1, \ldots, u_n) \mid f, g \in K[x_1, \ldots, x_n],\ u_1, \ldots, u_n \in X,\ g(u_1, \ldots, u_n) \neq 0,\ n \in \mathbb{N}\}.
\end{aligned}$$

Note: For the last two formulas, we could try to write each element as polynomials in an infinite number of variables, but this becomes much less workable.

Definition: Let $K \subseteq F$ be a field extension, and let $u \in F$. We say that u is algebraic over K if there exists some $f(x) \in K[x]$ with $f \neq 0$, such that $f(u) = 0$. We say that u is transcendental if u is not algebraic.

Note: Don't think of the elements of $K(x_1, \ldots, x_n)$ as actual functions. Just think of them as purely fractions of elements of the integral domain $K[x_1, \ldots, x_n]$. For example: in $\mathbb{F}_2[x]$, the functions $x^2 - x$ and 0 are equal, however they are completely different elements in the field.

Example: (Exercise V.1.6) If $f \in K(x_1, \ldots, x_n)$ and $f \notin K$, then f is transcendental over K. (Hint: the variables $x_1, \ldots, x_n$ are transcendental over K, so use contradiction.)

Definition: $K \subseteq F$ is called a simple extension if and only if there exists $u \in F$ such that $F = K(u)$.

Definition: $K \subseteq F$ is called a finitely generated extension if and only if there exist $u_1, \ldots, u_n \in F$ such that $F = K(u_1, \ldots, u_n)$.

Remark: Be aware of the different notions of "finiteness" for a field extension $K \subseteq F$:

(i) F is finite (and so K is finite).

(ii) F is finite dimensional as a vector space over F, sometimes referred to as a "finite extension".

(iii) $F = K(u_1, \ldots, u_n)$, so F is "finitely generated" over K.

Example: $F = K[x]$ is (iii) but not (ii).

Theorem V.1.5: If $K \subseteq F$ and $u \in F$ is transcendental over K, then $K(u) \cong K(x)$, the field of rational functions in one variable, by an isomorphism taking $x \mapsto u$ and which is the identity on K.

Proof: By the **Universal Mapping Property of Polynomial Rings** on $K[x]$, there exists a unique homomorphism

$$\varphi : K[x] \to F,$$

mapping $x \mapsto u$ and which is the identity on K.

Since u is transcendental, we have that φ is injective: [$\operatorname{Ker}\varphi = \{$ polynomials that send x to 0 $\}$. Since u is transcendental, $f(u) \neq 0$ if $f \neq 0$. So $\operatorname{Ker}\varphi$ is trivial, and thus φ is injective.]

Since $K(x)$ is the field of fractions of $K[x]$, we can extend φ to a homomorphism $\widetilde{\varphi} : K(x) \to F$, and since $K(x)$ is generated over K by x, it is clear that $\operatorname{Im}\varphi$ is generated over K by $\widetilde{\varphi}(x) = u$, i.e., $\operatorname{Im}\widetilde{\varphi} = K(u)$. $\square$

Note: By using the **Universal Mapping Property of Polynomial Rings**, we avoid needing to check that φ was well-defined, a homomorphism, etc, since all of these properties hold automatically.

Theorem V.1.6: Let $K \subseteq F$ be a field extension and suppose $u \in F$ is algebraic over K.

(1) $K(u) = K[u]$;

(2) $K(u) \cong K[x]/(f)$, where $f \in K[x]$ is an irreducible monic polynomial of degree $n \geq 1$ uniquely determined by the conditions that $[f(u) = 0]$ and $[g(u) = 0$, with $g \in K[x]$, if and only if f divides $g]$;

(3) $\big[K(u) : K\big] = n$;

(4) $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K;

(5) Every element of $K(u)$ can be written uniquely in the form $a_0 + a_1 u + \ldots + a_n u^{n-1}$, with $a_j \in K$.

Proof: Consider the homomorphism $\varphi : K[x] \to F$ that maps $x \mapsto u$ and is the identity on K. This exists uniquely by the **Universal Mapping Property of Polynomial Rings**. Since u is algebraic, we have that $\operatorname{Ker}\varphi \neq 0$. Since $K[x]$ is a Principal Ideal Domain, we can pick f to be the monic generator of minimal degree of $\operatorname{Ker}\varphi$, so that $\operatorname{Ker}\varphi = (f)$. We can pick it to be monic because K is a field, so we can set the leading coefficient to 1.

We claim that f is irreducible. If f is not irreducible, then let g, h be such that $f = gh$, where $\deg g < \deg f$. Then, $0 = f(u) = g(u)h(u)$. Since $K[x]$ is an integer domain, either $g(u) = 0$ or

$h(u) = 0$. But then, f is not the polynomial with minimal degree that generated $\operatorname{Ker}\varphi$. This is a contradiction. Thus f is irreducible.

Now, $\operatorname{Im}\varphi = K[u]$. Since f is irreducible, the ideal (f) is a maximal ideal. Thus $\operatorname{Im}\varphi$ is a field. So, $K[u]$ is a field. Thus $K[u] = K(u)$, and so (1) and (2) are proved.

Next we claim that $K[u]$ is generated by $\{K, u, u^2, \ldots, u^{n-1}\}$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Since $f(u) = 0$, we have that

$$-u^n = a_{n-1}x^{n-1} + \cdots + a_1u + a_0.$$

So, $K[u]$ is generated by $\{1, u, \ldots, u^{n-1}\}$. Thus the set spans $K[u]$. It remains to show that that set is linearly independent.

If $\{1, u, \ldots, u^{n-i}\}$ with $i > 1$ spans $K[u]$, then those elements form a polynomial for which $f(u) = 0$, contradicting the minimality of the degree of f. Thus, the set is linearly independent, and so it is a basis for $K[u]$. Thus (4) is proved.

(3) follows immediately from the construction of (4) and the statement [(4) $\Rightarrow$ (5)] is a routine vector space result. $\square$

Definition: Let F be an extension of K and let $u \in F$. Then,

$$K(u) \cong \begin{cases} K(x), & \text{if } u \text{ is transcendental,} \\ K[x]/(f), & \text{if } u \text{ is algebraic, for some monic irreducible} \\ & \text{polynomial } f, \text{ where } \deg f = n = |K(u) : K|. \end{cases}$$

This f is called the minimal polynomial of u over K.

Remark: Consider the following diagram:

$$\begin{array}{ccc} u \in F & & E \ni v \\ \cup & & \cup \\ K & \cong & L \end{array}$$

In this case, $\sigma : K \to L$ induces an isomorphism $\widetilde{\sigma} : K[x] \to L[x]$, such that

$$\widetilde{\sigma}(x) = x, \quad \widetilde{\sigma}(k) = \sigma(k).$$

Theorem V.1.8: If [u and v are transcendental] or if [u is a root of a non-zero irreducible polynomial $f \in K[x]$ and v is a root of $\sigma \circ f \in L[x]$], then there exists an isomorphism $\widetilde{\sigma} : K(u) \xrightarrow{\widetilde{\sigma}} L(v)$ extending σ.

Proof: Consider the following diagram:

$$\begin{array}{ccc} F & & E \\ \cup & & \cup \\ K[x] & \cong & L[x] \\ \cup & & \cup \\ K & & L \end{array}$$

In the case that u and v are transcendental, we have an embedding of σ to $K(u) \cong K(x)$, as above.

In the algebraic case:

$$\begin{array}{ccc} F & & E \\ \cup & & \cup \\ K[x]/(f) & \cong & L[x]/(\sigma \circ f) \\ \cup & & \cup \\ K & & L \end{array}$$

We use the same technique of embedding σ through a series of three isomorphisms.

Definition: If E, F are extensions of K, then a K-homomorphism from E to F is a field homomorphism which is the identity on K.

Theorem V.1.10: If K is a field and $f \in K[x]$ is a polynomial of degree n, then there exists a simple extension $F = K[u]$ such that:

(1) $u \in F$ is a root of f,

(2) $\big[K(u) : K\big] \leq n$ with equality if and only if f is irreducible,

(3) If f is irreducible, then $K(u)$ is unique up to K-isomorphism.

Proof: (Sketch) If f is reducible, then pick f_1 to be an irreducible factor of f. Then, (f_1) is a maximal ideal in $K[x]$. Thus, $K[x]/(f_1)$ is a field extension of K. Now, $K[x]/(f_1) = K(u)$, where $u := x + (f_1)$. Also, we know that $\big[K(u) : K\big] = \deg f$, with the basis $\{1, u, \ldots, u^{n-1}\}$.

Definition: An extension $K \subset F$ is an algebraic extension if every element of F is algebraic over K.

Definition: An extension $K \subset F$ is a transcendental extension if there exists an element of F which is transcendental over K.

Theorem V.1.11: If F is finite dimensional over K then F is finitely generated and algebraic over K.

Proof: (Sketch) Finite dimensional extension means that F is finite dimensional vector space over K. F has a finite basis by finite dimensionality. This basis spans F. So, F is finitely generated by this finite bases over K.

Take an element $u \in F$ which is n-dimensional and consider $\{1, u, \ldots, u^n\}$, a total of $n + 1$ elements. Thus, these elements are linearly dependent, and we can write u as a combination of the other elements. Thus u is algebraic, for any arbitrary $u \in F$. $\square$

Theorem V.1.12: If $F = K(X)$ for some $X \subset F$ and every element of X is algebraic over K, then F is an algebraic extension over K. If X is finite, then F is finite dimensional.

Proof: (Sketch) Let $\alpha \in F$. Then there exist finitely many elements $u_1, \ldots, u_r \in X$ such that $\alpha \in K(u_1, \ldots, u_r)$. The extension $K \subset K(u_1)$ is a finite extension since u_1 is algebraic over K. Similarly, the extension $K(u_1) \subset K(u_1, u_2)$ is a finite extension for the same reason. So, the extension $K \subset K(u_1, u_2)$ is algebraic over K. Continuing this process, we see that $K(u_1, \ldots, u_r)$ is a finite dimensional extension of K. $\square$

Theorem V.1.13: If $K \subset E \subset F$ and E is algebraic over K and F is algebraic over E, then F is algebraic over K.

Proof: Let $\alpha \in F$. Since α is algebriac over E, it satisfies some nonzero polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in E[x]$. Thus, α is algebraic over $K(a_0, \ldots, a_n)$. But, each of $a_0, \ldots, a_n$ is algebraic over K, so that $K(a_0, \ldots, a_n)$ is a finite extension (i.e. $|K(a_0, \ldots, a_n) : K| < \infty$).

By a previous theorem: $|K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)| < \infty$. Hence, $|K(a_0, \ldots, a_n)(\alpha) : K| < \infty$. Thus α is algebraic over K. $\square$

Theorem V.1.14: Let $K \subset F$ be a field extensions. Then $E := \{u \in F \mid u \text{ is algebraic over } K\}$ is a subfield of F.

> **Proof:** If $\alpha, \beta \in E$, then $K(\alpha)$ is algebraic over K and $K(\alpha, \beta)$ is algebraic over $K(\alpha)$. So, $K(\alpha, \beta)$ is algebraic over K. Now, $\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha\beta^{-1}$ (if $\beta \neq 0$) $\in K(\alpha, \beta)$. $\square$

Definition: In the theorem above, E is called the algebraic closure of K in F.

Special Topic: Ruler and Compass Constructions

Definition: Let F be a subfield of $\mathbb{R}$. L is a line of F if it passes through points $(a_1, b_1), (a_2, b_2)$, with $a_1, b_1, a_2, b_2 \in F$.

Definition: Let F be a subfield of $\mathbb{R}$. C is a circle of F if it is centered at a point (a, b) and has a radius r, with $a, b, r \in F$.

Lemma: Let F be a subfield of R.

(a) If L_1 and L_2 are lines of F, then their point of intersection, if it exists, has coordinates in F.

(b) The intersection points of a line of F and a circle of F have coordinates in $F(u)$, where $\big[F(u) : F\big] \leq 2$.

(c) The intersection points of two circles of F have coordinates in $F(u)$, where $\big[F(u) : F\big] \leq 2$.

Corollary: Any length c which can be constructued in a finite number of steps gives an extension field F of $\mathbb{Q}$ such that $\big[F : \mathbb{Q}\big] = 2^n$, for some $n \in \mathbb{N}$.

Example: The length $\sqrt[3]{2}$ is a root of $x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$ be Eisenstein's Criterion. Hence $\big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 3$. Thus $\sqrt[3]{2}$ is not a constructible length. So, constructing the length of the side of a cube which has volume 2 is not possible.

Example: Since π is transcendental, it's exists only in non-finite extensions of $\mathbb{Q}$. Thus it is not a constructible length. So, "squaring the circle" is not possible.

Example: We show that it is not possible to trisect the angle. With some trig, we get that

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$

Let $\theta = \dfrac{\pi}{9}$, so that $\cos(3\theta) = \dfrac{1}{2}$. Now, $\dfrac{1}{2} = 4x^3 - 3x$.

This has no rational root, and so its roots have field extensions of degree 3. Thus the length $\cos\left(\dfrac{\pi}{9}\right)$ and hence the angle $\dfrac{\pi}{9}$ are not constructible.

1.1.2 Section V.2 - The Fundamental Theorem

Definition: Let $K \subset F$. Then, $\mathrm{Aut}_K(F) := \{\sigma \in \mathrm{Aut}(F) \mid \sigma \mid_K = id_K\}$. We call this group the Galois group of F over K.

Note: Automorphisms of a field F are automatically injective if they're non-zero, since there are no non-trivial ideals for the kernel to be. However, surjectivity does not come for free.

Example: Consider $\varphi : \mathbb{F}_2(x) \to \mathbb{F}_2(x)$ defined by $\varphi(x) = x^2$. The same thing on the polynomial ring $\psi : \mathbb{F}_2[x] \to \mathbb{F}_2[x] \subset \mathbb{F}_2(x)$ is a homomorphism by the **Universal Mapping Property**. This is then a homomorphism into the superset $\mathbb{F}_2(x)$. If an integral domain has a homomorphism into a field of fractions, then its field of fractions also has a homomorphism into the field of fractions which, when restricted to the integral domain, is the first homomorphism. So, $\varphi : \frac{f(x)}{g(x)} \longmapsto \frac{f(x^2)}{g(x^2)}$, and so we see that φ is not surjective. Thus φ is not an automorphism: $\varphi \notin \mathrm{Aut}_{\mathbb{F}_2} \mathbb{F}_2(x)$.

Example: On the other hand, for K any field, let $\sigma_a : K(x) \to K(x)$ defined by $x \mapsto ax$, for $a \neq 0$. Now, in this case, by the same reasoning above, $\frac{f(x)}{g(x)} \mapsto \frac{f(ax)}{g(ax)}$. Clearly σ_a is surjective. Therefore, $\sigma_a \in \mathrm{Aut}_K K(x)$. Additionally, since K is infinte, so is $\mathrm{Aut}_K K(x)$.

Example: Similarly, the map $\tau_b : K(x) \to K(x)$ defined by $x \mapsto x + b$ is an automorphism. Again, by the **Universal Mapping Property**, the map $x \mapsto x+b$ is a homomorphism on the polynomial ring $K[x]$, and so its a homomorphism from $K[x]$ into $K(x)$, and thus it induces a map from $K(x)$ to $K(x)$. This induced map is $\frac{f(x)}{g(x)} \mapsto \frac{f(x+b)}{g(x+b)}$, which is surjective. Thus τ_b is an automorphism that is fixed on K, and so $\tau_b \in \mathrm{Aut}_K K(x)$.

Note: In the examples above, if $a \neq 1$ and $b \neq 0$, then $\sigma_a\tau_b(x) = ax + ab$ and $\tau_b\sigma_a = ax + b$. Thus, $\mathrm{Aut}_K K(x)$ is not abelian.

Theorem V.2.2: Let $K \subset F$ and $f(x) \in K[x]$, and let $u \in F$ be a root of f. Then, for all $\sigma \in \mathrm{Aut}_K(F)$, it is true that $\sigma(u)$ is also a root of f.

Proof: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Since u is a root of $f(x)$, we have that:

$$a_n u^n + \cdots + a_1 u + a_0 = 0.$$

Applying σ to both sides:

$$\sigma(a_n u^n + \cdots + a_1 u + a_0) = \sigma(0).$$

Since σ is a homomorphism:

$$\sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) = 0.$$

Since σ is the identity on K:

$$a_n\sigma(u)^n + \cdots + a_1\sigma(u) + a_0 = 0.$$

Therefore, $\sigma(u)$ is a root of f. □

Remark: If a polynomial is *reducible*, then an automorphism σ moves roots only within the same *irreducible* factors, but not between them.

Example: Let $F = K$. Then, $\mathrm{Aut}_K F = \{\mathrm{Id}_F\} =: 1$.

Example: Consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. Now, $\mathrm{Aut}_{\mathbb{Q}}(\sqrt[3]{2}) = 1$, since $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$. So, since any automorphism σ maps $\sqrt[3]{2}$ to another root of $x^3 - 2$, we have that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Because σ is already the identity on $\mathbb{Q}$, we have that σ is the identity on all of $\mathbb{Q}(\sqrt[3]{2})$.

Example: Consider $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i)$. Any automorphism that is the identity on $\mathbb{R}$ is determined completely by where it sends i to. It must send i to another root of $x^2 + 1 = 0$. So, the two possibilities are:

$$i \mapsto i,$$

$$i \mapsto -i.$$

The first is the identity and is obviously an automorphism.

We must show that $i \mapsto -i$ is really an automorphism. If it is, then $|\operatorname{Aut}_{\mathbb{R}} \mathbb{C}| = 2$, so $\operatorname{Aut}_{\mathbb{R}} \mathbb{C} \cong Z_2$. A routine verification shows that $i \mapsto -i$ is indeed an automorphism.

Theorem V.2.3: Let $K \subset F$. Let E be an intermediate field, and let H be a subgroup of $\mathrm{Aut}_K F$.

(i) $H' := \{v \in F \mid \sigma(v) = v, \text{ for all } \sigma \in H\}$ (called the fixed field of H) is a field containing K.

(ii) $E' := \{\sigma \in \mathrm{Aut}_K F \mid \sigma(u) = u, \text{ for all } u \in E\} = \mathrm{Aut}_E F$ is a subgroup of $\mathrm{Aut}_K F$.

Definition: Let F be an extension of K such that the fixed field of $\mathrm{Aut}_K F$ is equal to K (i.e. $(\mathrm{Aut}_K F)' = K$). Then we call F a Galois Extension of K and say that F is Galois over K.

Counterexample: Let $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$. Then, $\mathbb{Q}' = 1$, and $1' = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$. So, $\mathbb{Q}(\sqrt[3]{2})$ fails to be a Galois Extension of $\mathbb{Q}$.

Remark: For F to be a Galois Extension over K, you have to have "enough" automorphisms to move every element not in K to somewhere else.

Example: $\mathbb{C}$ is Galois over $\mathbb{R}$. $\mathbb{Q}(\sqrt{3})$ is Galois over $\mathbb{Q}$. $K(x)$ is Galois over K.

Fundamental Theorem of Galois Theory: If f is an finite dimensional Galois extension of K, then there is an inclusion reversing one-to-one correspondence between the set of all intermediate fields an the set of all subgroups of $\mathrm{Aut}_K(F)$, such that:

$$E \longmapsto E' = \mathrm{Aut}_E F$$
$$H' \longleftarrow\!\shortmid H.$$

Additionally,

(i) The relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups.

(ii) [F is Galois over every intermediate field E], but [E is Galois over K if and only if $\mathrm{Aut}_E F \trianglelefteq \mathrm{Aut}_K F$]. In this case $\mathrm{Aut}_K F / \mathrm{Aut}_E F \cong \mathrm{Aut}_K E$.

Remark: If $K \subset L \subset M \subset F$, then $\mathrm{Aut}_K F \supset \mathrm{Aut}_L F \supset \mathrm{Aut}_M F \subset \mathrm{Aut}_F F = 1$.

Lemma V.2.6: Let $G = \mathrm{Aut}_K F$.

(i) $F' = 1$, $K' = G$.

(ii) $1' = F$.

(iii) $L \subset M \Longrightarrow M' \subset L'$.

(iii') $H \subset J \Longrightarrow J' \subset H'$.

(iv) $L \subset L''$ and $H \subset H''$

(v) $L' = L'''$ and $H' = H'''$

Proof of (v): $L' \subset (L')'' = L'''$ by (iv). If you take $L \subset L''$ and $'$ each side, it reverses the inclusion, so $L' \supset L'''$. $\square$

Definition: We say an intermediate field M is closed if $M = M''$. We say a subgroup H of G is closed if $H = H''$.

Theorem V.2.7: Let F be an extension field of K. Then, there is a one-to-one correspondence between the closed subgroups of $\mathrm{Aut}_K F$ and the closed intermediate fields given by

$$E \to E' = \mathrm{Aut}_E F.$$

Lemma V.2.8: Let $K \subset L \subset M \subset F$. If $\big[M : L\big]$ is finite, then $\big[L' : M'\big] \leq \big[M : L\big]$. In particular, if $\big[F : K\big]$ is finite, then $|\mathrm{Aut}_K F| \leq \big[F : K\big]$.

Proof: (by induction on $n = \big[M : L\big]$) If $n = 1$, then $M = L$ and the proof is trivial. Assume $n > 1$. Let $u \in M \setminus L$. Let $k := \big[L(u) : L\big]$. If $k < n$, then by induction we have that $\big[L' : L(u)'\big] \leq k$, and $\big[L(u)' : M'\big] \leq \frac{n}{k}$. Hence, $\big[L' : M'\big] = \big[L' : L(u)'\big]\big[L(u)' : M\big] \leq k \cdot \frac{n}{k} = n$.

So, assume now that $k = n$, i.e. $L(u) = M$. Let $f \in L[x]$ be the minimal polynomial of u. Let X be the set of roots of f that lie in F. Then, $L' = \mathrm{Aut}_L F$ acts on the set of roots X and $M' = \mathrm{Aut}_M F = \mathrm{Aut}_{L(u)} F$ is the stabilizer of u in L'.

By the **Orbit-Stabilizer Theorem**, we have a bijection between the cosets of M' in L' and the orbit of u under the action of L'. Hence $\big[L' : M'\big] \leq |X| \leq \deg f = \big[M : L\big]$. $\square$

Lemma V.2.9: Let $K \subset F$ be an extension and let $H, J \leq G = \mathrm{Aut}_K F$ with $H < J$. If $\big[J : H\big]$ is finite, then $\big[H' : J'\big] \leq \big[J : H\big]$.

Proof: Let $n = \big[J : H\big]$. Suppose toward a contradiction that $\big[H' : J'\big] < n$. Then, there exist $u_1, \ldots, u_{n+1} \in H'$ that are linearly independent over J'. Let $\tau_1, \ldots, \tau_n$ be coset representatives of H in J, i.e. $J = \bigcup_{i=1}^{n} \tau_i H$.

Consider the system of equations:

$$\begin{aligned}
\tau_1(u_1)x_1 + \tau_1(u_2)x_2 + \cdots + \tau_1(u_{n+1})x_{n+1} &= 0,\\
\tau_2(u_1)x_1 + \tau_2(u_2)x_2 + \cdots + \tau_2(u_{n+1})x_{n+1} &= 0,\\
&\vdots\\
\tau_n(u_1)x_1 + \tau_n(u_2)x_2 + \cdots + \tau_n(u_{n+1})x_{n+1} &= 0.
\end{aligned}$$

Since the system has n equations in $n + 1$ variables, it has non-trivial solutions.

By renumbering if necessary, pick one $(a_1, \ldots, a_{n+1})$ such that $a_1 = 1$ (by making $a_1 \neq 0$ and dividing) and such that the number r of nonzero entries is minimal among all nonzero solution. By renumbering, write the solution so that all nonzero entries come first:

$$a_1, \ldots, a_r \neq 0, \qquad a_{r+1}, \ldots, a_{n+1} = 0.$$

The idea is to find a "shorter" nontrivial solution, we pick $\sigma \in J$ such that $\sigma(a_1) = 1$ and $\sigma(a_2) \neq a_2$ and such that $(\sigma(a_1), \ldots, \sigma(a_r), 0, \ldots, 0)$ is also a solution. By subtracting the above solution from $(a_1, \ldots, a_{n+1})$, we get a nonzero solution with at least one additional zero (since $\sigma(a_1) - a_1 = 1 - 1 = 0$ and $\sigma(a_2) - a_2 \neq 0$).

Without loss of generality, let $\tau_1 \in H$. So, the first equation has

$$u_1 + u_2 a_2 + \cdots + u_{n+1} a_{n+1} = 0.$$

Thus since the u_i are linearly independent over J', we must have some $a_j \notin J'$ (otherwise all $a_i = 0$, which is not true). Without loss of generality, let $a_2 \notin J'$. Then there exists $\sigma \in J$ such that $\sigma(a_2) \neq a_2$.

Now consider the above system of equations with each τ_i replaced by $\sigma\tau_i$.

$$[\sigma\tau_1]u_1)x_1 + [\sigma\tau_1](u_2)x_2 + \cdots + [\sigma\tau_1](u_{n+1})x_{n+1} = 0,$$

$$[\sigma\tau_2](u_1)x_1 + [\sigma\tau_2](u_2)x_2 + \cdots + [\sigma\tau_2](u_{n+1})x_{n+1} = 0,$$

$$\vdots$$

$$[\sigma\tau_n](u_1)x_1 + [\sigma\tau_n](u_2)x_2 + \cdots + [\sigma\tau_n](u_{n+1})x_{n+1} = 0.$$

Each τ_i is a left coset representative of H in J. So, J acts on the set of left cosets of H by left multiplication:

$g : \tau_i H \mapsto (g\tau_i)H = \tau_{i'}H$, for some i'. Note that $g \in J$.

Hence the set $\{g\tau_i\}_{i=1}^n$ is also a set of left coset representatives, for each $g \in J$. In particular, the set $\{\sigma\tau_i\}_{i=1}^n$ is a set of left coset representatives. So,

$$\sigma\tau_i = \tau_{\pi(i)} h_i \text{ for some permutation } \pi \in S_n, \text{ and } h_i \in H.$$

Then, $(\sigma\tau_i)(u_j) = (\tau_{\pi(i)}h_i)(u_j) = \tau_{\pi(i)}(h_i u_j) = \tau_{\pi(i)}(u_j)$. So, the second system of equations is the same as the first system of equations, except with the order of the equations permuted by π.

Since σ is a field automorphism and $a_1, \ldots, a_{n+1}$ is a solution of the original system of equations, we have that $(\sigma(a_1), \ldots, \sigma(a_{n+1}))$ is a solution of the new system. But since we know that the two systems are equal, the set of solutions to each is the same. But, we picked $(a_1, \ldots, a_{n+1})$ to have r be the minimal number of nonzero elements, and the solution $(\sigma(a_1), \ldots, \sigma(a_{n+1}))$ has one less nonzero element. This is a contradiction. Therefore $\big[H' : J'\big] \leq n$. $\square$

Lemma V.2.10:

(i) If L is closed and $\big[M : L\big] < \infty$, then M is closed and $\big[L' : M'\big] = \big[L : M\big]$, i.e. "Any finite extension of a closed field is closed."

(ii) If H is closed and $\big[J : H\big] < \infty$, then J is closed and $\big[H' : J'\big] = \big[J : H\big]$.

(iii) If F is a finite dimensional Galois extension of K, then all intermediate fields are closed, and all corresponding automorphism subgroups are closed, and $|\operatorname{Aut}_K F| = \big[F : K\big]$.

Proof of (i): We want to show that $M = M''$. It's always true that $M \subseteq M''$. Thus $\big[M : L\big] \leq \big[M'' : L\big]$. Since L is closed, $L = L''$ and thus $\big[M : L\big] \leq \big[M'' : L''\big]$. By **Lemma 2.9**, $\big[M'' : L''\big] \leq \big[L' : M'\big]$. By **Lemma 2.8**, $\big[L' : M'\big] \leq \big[M : L\big]$. So,

$$\big[M : L\big] \leq \big[M'' : L\big] = \big[M'' : L''\big] \leq \big[L' : M'\big] \leq \big[M : L\big].$$

Thus we have equality throughout, and so $M = M''$ and $\big[L' : M'\big] = \big[M : L\big]$. □

Proof of (ii): Similarly, $\big[J : H\big] \leq \big[J'' : H\big] = \big[J'' : H''\big] \leq \big[H' : J'\big] \leq \big[J : H\big]$. So, we have equality throughout, thus $J = J''$ and $\big[H' : J'\big] = \big[J : H\big]$. □

Proof of (iii): If F is a finite dimensional Galois extension, then that means $K = K''$, and $1 = 1''$ whether or not F is Galois. Apply **(i)** with $M := F$ and $L := K$. All intermediate fields will also be finite dimensional so they'll definitely be closed. See book for details. □

To say that F is Galois over an intermediate field M means that $M'' = M$ (i.e., for every element not in M, there is an automorphism in $\mathrm{Aut}_M F$ that moves it somewhere else). We'd like to be able to say something about if F is Galois over K then is L (where $F \subset L \subset K$) Galois over K?

This is the only part left to show of the Fundamental Theorem:

If F is Galois over K, then $L \supset K$ is Galois if and only if $L' \trianglelefteq G$, and if so, then $\mathrm{Aut}_K L \cong G/L'$.

Definition: Let $K \subset E \subset F$. We say that E is <u>stable relative to $K \subset F$</u> if for all $\sigma \in \mathrm{Aut}_K F$, we have that $\sigma(E) \subseteq E$.

Lemma V.2.11: Assume E is stable. Then,

(1) $E' = \mathrm{Aut}_E F$ is a normal subgroup of $\mathrm{Aut}_K F$.

(2) If $H \trianglelefteq \mathrm{Aut}_K F$ then H' is stable.

Proof of (i): Let $\tau \in \mathrm{Aut}_E F$ and $\sigma \in \mathrm{Aut}_K F$, and let $u \in E$. Then, $\sigma\tau\sigma^{-1}(u) = \sigma(\tau\sigma^{-1}(u)) = \sigma(\sigma^{-1}(u))$, since $\sigma^{-1}(u) \in E$ by stability, and since τ fixes E. Thus $\sigma\tau\sigma^{-1}(u) = u$. Hence $\sigma\tau\sigma^{-1} \in \mathrm{Aut}_E F$. □

Proof of (ii): Let $u \in H'$ and let $\sigma \in \mathrm{Aut}_K F$ and let $\tau \in H$. Since $H \trianglelefteq \mathrm{Aut}_K F$, we have $\tau\sigma = \sigma\tau'$ for some $\tau' \in H$. So, $\tau(\sigma(u)) = \sigma(\tau'(u)) = \sigma(u)$ for some $u \in H'$ and $\tau' \in H$. Therefore $\sigma(u) \in H'$. □

Lemma V.2.12: If F is Galois over K and E is a stable intermediate field, then E is Galois over K. (We know that F is Galois over its intermediate fields, but we don't know yet when the intermediate fields are Galois over K.)

Proof: Let $u \in E \setminus K$. We will find an element $\sigma \in \mathrm{Aut}_K E$ such that $\sigma(u) \neq u$. Since F is Galois over K, there exists $\sigma \in \mathrm{Aut}_K F$ such that $\sigma(u) \neq u$, since $u \in F \setminus K$. Then, since E is stable, we have that the $\sigma\big|_E \in \mathrm{Aut}_K E$, and now $\sigma\big|_E(u) \neq u$. Hence E is Galois over K. □

Lemma V.2.13: Let $K \subset E \subset F$. If E is algebraic over K and E is Galois over K, then E is stable over K.

Proof: Let $u \in E$, $\sigma \in \operatorname{Aut}_K F$. We have to show that $\sigma(u) \in E$. Let $f(x) \in K[x]$ be the minimal polynomial of u. Let $u = u_1, u_2, \ldots, u_n$ be the distinct roots of $f(x)$ in E. Let $g(x) := (x - u_1)(x - u_2) \cdots (x - u_n) \in E[x]$.

Then, $\operatorname{Aut}_K E$ permutes the set $\{u_1, \ldots, u_n\}$. So, $\operatorname{Aut}_K E$ fixes $g(x)$. But, E is Galois over K. Thus $g(x) \in K[x]$. Hence $f(x) \mid g(x)$. On the other hand, $\deg f \geq \#$ of roots in E. So, $f(x) = g(x)$. Hence all roots of $f(x)$ lie in E. Therefore, $\sigma(u) \in E$, so E is stable. $\square$

Definition: We say that $\tau \in \operatorname{Aut}_K E$ is extendable to F if there exists $\sigma \in \operatorname{Aut}_K F$ such that $\sigma\big|_E = \tau$. The extendable automorphisms form a subgroup.

Lemma V.2.14: If E is a stable intermediate field, then ($\operatorname{Aut}_E F \trianglelefteq \operatorname{Aut}_K F$, from a previous lemma) and

$$\operatorname{Aut}_K F / \operatorname{Aut}_E F \cong \text{ [the subgroups of extendible automorphisms in } \operatorname{Aut}_K E.]$$

Proof: E is stable, so we have a map $\operatorname{Aut}_K F \xrightarrow{\text{by domain restriction}} \operatorname{Aut}_K E$, and the image of that map is the subgroup of extensible automorphism, by definition. Additionally, the kernel of that map is $\{\sigma \in \operatorname{Aut}_K F \mid \sigma\big|_E = \mathrm{Id}\} = \operatorname{Aut}_E F$. $\square$

Part (ii) of Fundamental Theorem: E is Galois over K if and only if $E' \trianglelefteq G$.

Proof:

($\Longrightarrow$) : Suppose E is Galois over K. E is finite dimensional over K, hence algebraic. So E is stable by **Lemma 2.13**, thus $E' \trianglelefteq G$ by **Lemma 2.1(i)**. $\square$

($\Longleftarrow$) : Suppose E' is normal in $\operatorname{Aut}_K F$. Then E'' is stable by **Lemma 2.13**. But all intermediate fields are closed, so $E = E''$. By **Lemma 2.12**, E is Galois over K. $\square$

Proof of part of part (iii) of Fundamental Theorem: Assume that $E' \trianglelefteq G$, i.e. E is Galois over K, and E is stable. By part of **Lemma 2.14**, we have that $\operatorname{Aut}_K F / \operatorname{Aut}_E F \cong$ [extendible automorphisms] $\leq \operatorname{Aut}_K E$ (†). By their relative degrees, $|\operatorname{Aut}_K F| = |\operatorname{Aut}_E F| \cdot |\operatorname{Aut}_K E|$, since $\big[F : K\big] = \big[F : E\big] \cdot \big[E : K\big]$. So, we must have equality in (†). Thus $\operatorname{Aut}_K F / \operatorname{Aut}_E F \cong \operatorname{Aut}_K E$. $\square$

Theorem V.2.15: (Artin) Let F be a field and let G be a group of automorphisms of F. Let K be the fixed field of G. Then, F is Galois over K. If $|G| < \infty$, then F is finite dimensional and $\operatorname{Aut}_K F = G$.

Proof: Let $u \in F \setminus K$. Then, there exists $\sigma \in G$ such that $\sigma(u) \neq u$. Thus F is Galois over K. Suppose G is finite. Then, $F = 1'$, and $K = G'$, and $\big[F : K\big] = \big[1' : G'\big] \leq \big[G : 1\big] = |G|$. Thus F is a finite dimensional Galois extension of K, and $|\operatorname{Aut}_K F| = \big[F : K\big] \leq |G|$, so $\operatorname{Aut}_K F = G$. $\square$

Special Topic: Symmetric Rational Functions

Consider the symmetric group S_n and the polynomial ring $K[x_1, \ldots, x_n]$.

For each $\sigma \in S_n$ and $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, let

$$(\sigma f)(x_1, \ldots, x_n) := f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Then, the map $\widetilde{\sigma} : f \mapsto \sigma f$ is an automorphism on $K[x_1, \ldots, x_n]$.

The map $\Phi : S_n \to \mathrm{Aut}_K(K[x_1, \ldots, x_n])$ defined by $\sigma \mapsto \widetilde{\sigma}$ is a homomorphism. To see this, we check that $\Phi(\sigma\tau)(f) = (\widetilde{\sigma\tau})f = \widetilde{\sigma}(\widetilde{\tau}(f)) = \Phi(\sigma)\Phi(\tau)(f)$:

$$\begin{aligned}\widetilde{\sigma}(\widetilde{\tau}(f(x_1, \ldots, x_n))) &= \widetilde{\sigma}(f(x_{\tau(1)}, \ldots, x_{\tau(n)}) \\ &= f(x_{\sigma(\tau(1))}, \ldots, x_{\sigma(\tau(n))}) \\ &= f(x_{(\sigma\tau)(1)}, \ldots, x_{(\sigma\tau)(n)}) \\ &= (\widetilde{\sigma\tau})(f(x_1, \ldots, x_n)).\end{aligned}$$

Then, we get an induced action of S_n on $K(x_1, \ldots, x_n)$, the field of rational fractions. (An injective homomorphisms from an integral domain to an integral domain induces an injective homomorphism on the field of fractions of each the domain and the codomain. In our case, it's also surjective.)

The induced action is:

$$\sigma\left(\frac{f(x_1, \ldots x_n)}{g(x_1, \ldots, x_n)}\right) = \frac{f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{g(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}.$$

Now, we have a group acting on a field, resulting in the fixed subfield E of S_n on $K(x_1, \ldots, x_n)$, which is called the field of symmetric rational functions. [Recall that the fixed subfield consists of all the elements who are unchanged by applying all elements of S_n. In this case, it is all rational functions that are unchanged by reordering the indeterminates.] By **Artin's Theorem**, $E \subset K(x_1, \ldots, x_n)$ is Galois of degree $n!$ with Galois group S_n.

Let G be a finite group. By **Cayley's Theorem**, there exists n such that $G \cong$ [a subgroup of S_n]. Identity G with that subgroup.

Consider fields $K(x_1, \ldots, x_n) \supset F \supset E$ and corresponding groups $1 \subset G \subset S_n$.

Let F be the fixed field of G. Then, $K(x_1, \ldots, x_n)$ is Galois over F with Galois group G. (This shows that given any group G, we can find its fixed field, and a field extension of its fixed field which is Galois over the fixed field, with Galois group G.)

Elementary Symmetric Functions

Consider the variables, $x_1, \ldots, x_n$.

The first elementary symmetric function is

$$f_1 = x_1 + \cdots + x_n = \sum_{i=1}^{n} x_i.$$

The second elementary symmetric function is

$$f_2 = \sum_{1 \le i < j \le n} x_i x_j.$$

The thid elementary symmetric function is

$$f_3 = \sum_{1 \le i < j < k \le n} x_i x_j x_k.$$

Finally, the n^{th} symmetric function is just

$$f_n = x_1 x_2 \cdots x_n.$$

To see that they're symmetric, consider $K(x_1, \ldots, x_n)[y]$ with the polynomial

$$(y - x_1) \cdots (y - x_n) = y^n - f_1 y^{n-1} + f_2 y^{n-2} + \cdots + (-1)^n f_n.$$

Hence, each f_i is symmetric.

Remark: These roots relate to matrices. f_1 is the trace - the sum of the eigenvalues. f_n is the product of the eigenvalues. Each f_i makes up the coefficients of the characteristic polynomial. The study of these relationships dates at least back to Newton.

Theorem V.2.18: If K is a field, E the subfield of all symmetric rational functions in $K(x_1, \ldots, x_n)$ and $f_1, \ldots, f_n$ the elementary symmetric functions, then $E = K(f_1, \ldots, f_n)$. (So, the elementary symmetric functions generate the field of symmetric functions and the ring of symmetric polynomials. If you write down any symmetric polynomial (ex: $x_1^k + x_2^k + \cdots + x_n^k$), it's not immediately clear that it is a polynomial made up of elementary symmetric functions, but it is. The theorem is in fact even true if you replace K by $\mathbb{Z}$, which is an even stronger statement – Newton proved this.)

Proof: The proof is in the book. It is somewhat elementary, but has a complicated induction argument. It should be worked through individually. □

1.1.3 Section V.3 - Splitting Fields, Algebraic Closure, and Normality

Definition: Let $S \subset K[x]$ be a set. An extension E of K is a splitting field of S if and only if

(i) Every polynomial in S splits (i.e., factors into linear factors) over E, and

(ii) E is generated over K by the roots of the polynomials in S.

The first condition says that the splitting field is big enough to contain all roots of the polynomials, and the second condition says that the splitting isn't too big to contain unneeded things. If S is finite, then finding the splitting field of a bunch of polynomials is equivalent to finding the splitting field of the one polynomial which is product of those polynomials.

Theorem V.3.2: If K is a field and $f(x) \in K(x)$ has degree $n \geq 1$, then there is a splitting field F of f over K with $\big[F : K\big] \leq n!$.

> **Proof:** (by induction on $\deg f$) Let g be an irreducible factor of f. Adjoin a root u of g to K so that $K(u) = K[x]/(g)$. Now, the extension $K(u) \supset k$ has degree $\deg g \leq \deg f = n$. Then, in $K(u)[x]$, now f factors as $(x-u)f_1$, where $\deg f_1 = n - 1 < n$.
>
> By induction, there exists a splitting field E of f_1 over $K(u)$ of degree $\leq (n-1)!$. Now we need to check that:
>
> (1) E is a splitting field for f over K, and
>
> (2) $\big[E : K\big] \leq n!$.
>
> The second condition has just been shown, since $n \cdot (n-1)! = n!$. The first condition is true since $E = K(u)(r_1, \ldots, r_{n-1})$, where $r_1, \ldots, r_{n-1}$ are the roots in f_1 (by induction), so E is certainly the splitting field for f over K. $\square$
>
> [Note: one of the exercise has you show that the degree of the splitting field actually divides $n!$.]

Theorem V.3.3: The following are equivalent:

(1) Every nonconstant polynomial $f \in F[x]$ has a root in F.

(2) Every nonconstant polynomial $f \in F[x]$ splits in F.

(3) Every irreducible $f \in F[x]$ has degree 1.

(4) F has no algebraic extensions except itself.

(5) There exists a subfield K of F such that F is algebraic over K and every polynomial $f \in K[x]$ splits over F.

Definition: A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ has a root in F (i.e., if it satisfies the equivalent conditions of **Theorem V.3.3**. An extension field F of a field K is called an algebraic closure of K if F is algebraic over K and F is algebraically closed.

Theorem V.3.6: Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.

> **Remark:** This proof uses Zorn's Lemma. It is a tricky application, since the "set of all fields that are algebraic over K" is not a set (or we'd have the Russell Paradox). Rather, it's a proper class. (In this course, we use Von Neumann-Bernays-Gödel Set Theory.) For this proof, we find the set that has a "copy" of all fields that are algebraic over K (in the same way that $\mathbb{Z}$ does not contain all finite sets, but does contain a "copy" of all finite sets.

First we prove a lemma.

Lemma V.3.5: If F is an algebraic extension of K, then $|F| \leq \aleph_0|K|$.

Remark: $|F| \leq \aleph_0|K|$ means "If K is finite, then$|F| \leq \aleph_0$, and if K is infinite, then $|F| \leq |K|$." since

$$\aleph_0|K| = \begin{cases} \aleph_0, & K\text{is finite} \\ |K|, & K\text{is infinite} \end{cases}.$$

Proof: Let $T^n := \{\text{polynomials of degree } n \text{ over } K\}$. Then, $T^n \leq \underbrace{K \times \cdots \times K}_{n+1}$. If $|K| < \infty$, then clearly the number of polynomials over K is countable. Now assume that $|K|$ is infinite. Let T be the set of all polynomials over K. Then $|T| = \left|\bigcup_{n=0}^{\infty} T^n\right| \leq \aleph_0|K|$.

For each irreducible monic polynomial in $K[x]$ choose an ordering of its roots in F. Let $u \in F$. Let $f(x) \in K[x]$ be the minimal polynomial of u, with roots ordered $u_1, \ldots, u_{k(f)}$. Then $u = u_k$ for some j.

Define $F \to T \times \mathbb{N}$ by $u \mapsto (f(x), j)$. This is obviously an injective map, so $|F| \leq |T \times \mathbb{N}| = |T| \leq \aleph_0|K|$. $\square$

Consequence: The algebraic numbers in $\mathbb{R}$ are countable, and therefore transcendental numbers exist.

Proof: Now that we have shown this lemma, we can find a set not much bigger than K containing a copy of each algebraic extension of K. Let S be a set with $|S| > \aleph_0|K|$. We have an injective map $\theta : K \to S$, by cardinalities, so now identify K with a subset of S, i.e., assume $K \subset S$.

Let $\mathcal{S}$ be the class of all fields E such that $E \subset S$, and $K \subset E$ as fields, and E algebraic over K. We call $\mathcal{S}$ a class because we don't know if its actually a set yet. We show that $\mathcal{S}$ is a set by showing it's a subclass of some class that is already a set.

If $E \in \mathcal{S}$, then as a field, E is completely determined by:

(a) its set of elements,

(b) the multiplication operation, and

(c) the addition operation.

Note that (a) is a subset of $\mathbb{P}(S)$, and (b) and (c) are subsets of $\mathbb{P}(S \times S \times S)$. So, the field E is determined by a tuple (E, μ, α), for $E \in \mathbb{P}(S)$, $\mu, \alpha \in \mathbb{P}(S \times S \times S)$. Thus, we have an injective map:

$$\mathcal{S} \longrightarrow \mathbb{P}(S) \times \mathbb{P}(S \times S \times S) \times \mathbb{P}(S \times S \times S).$$

If S is a set then so is $\mathbb{P}(S)$, etc, and so is anything mapping injectively into a set. Hence $\mathcal{S}$ is a set. (Note that the hard part is not proving $\mathcal{S}$ is a set, but rather appreciating why it's necessary to prove that it is.)

Say that $E_1 \leq E_2$ if E_2 is a field extension of E_1. This forms a partial order. Thus $\mathcal{S}$ is partially ordered, and we know $\mathcal{S} \neq \emptyset$, since $K \in \mathcal{S}$. Given a chain, consider its union. That union is still a field, and each element of the union is in some chain element, and thus algebraic over K. Thus the union is an algebraic extension over K and is still in S, thus still in $\mathcal{S}$.

Hence the hypotheses of **Zorn's Lemma** are satisfied. Therefore, we conclude that $\mathcal{S}$ has a maximal element F.

Claim: F is algebraically closed.

Proof: Assume toward a contradiction that F is not algebraically closed. Then, there exists $f \in F[x]$ which is irreducible and has $\deg f > 1$. Let u be a root of f in some extension field, i.e., $u \notin F$. Consider the extension $F(u)$. Clearly, $F(u) \supsetneq F$. Since u is algebraic over F and F is algebraic over K, we have that u algebraic over K and hence $F(u)$ is algebraic over K. Thus $|F(u)| \leq \aleph_0|K| < |S|$. We still have that $|F| \leq \aleph_0|K| < |S|$.

So, the identity map of F can be extended to an injection ψ of $F(u)$ into S (since S is so much bigger than F and $F(u)$ that there is still room for $F(u)$ to be moved into S. Now, we can make $\psi(F(u))$ into a field using the operations of $F(u)$. Clearly, $\psi(F(u))$ is an algebraic extension of K inside S, so $\psi(F(u)) > F$. This contradicts maximality of F. So F is algebraically closed. □

The above proves that every field has an algebraic closure, but it still remains to show that any two algebraic closures are K-isomorphic. A corollary to this second part is that every polynomial has a splitting field contained in its algebraic closure, since the field generated by all roots of all polynomials becomes an algebraic closure and is thus isomorphic to the original algebraic closure.

Theorem V.3.8: Let $\sigma : K \to L$ be an isomorphism of fields, let S be a set of polynomials (of positive degree), and let $S' := \{\sigma f \mid f \in S\} \subseteq L[x]$. If F is a splitting field for S over K and M is a splitting field for S' over L, then σ can be extended to an isomorphism from F to M.

Proof: Suppose first that $S = \{f\}$. Now, $S' = \{\sigma f\}$. Note the assumption that $|S| = 1$ is equivalent to S being any finite set of polynomials, since the splitting field of a finite set of polynomials is equal to the splitting field of the one polynomial which is the product of all of the polynomials.

Let u be a root of f in F. Let g be an irreducible factor of f having u as a root. Let $u' \in M$ be the corresponding root of σg.

$$\begin{array}{rcc} F & & M \\ (\deg f_1 < \deg f) \cup & & \cup \\ K(u) & \xrightarrow{\widetilde{\sigma}} & L(u') \\ (\deg g > 1) \cup & & \cup \\ K & \xrightarrow{\sigma} & L \end{array}$$

Then, by an earlier theorem, σ extends to an isomorphism $\widetilde{\sigma} : K(u) \to L(u')$ defined by $u \mapsto u'$. (In fact, both $K(u)$ and $L(u')$ are isomorphic to $K[x]/(g)$.) In $K(u)$, $f = (x-u)f_1$, and in $L(u')$, $\sigma f = (x-u')\widetilde{\sigma} f_1$. To apply induction (on $\deg f$), we have to check that F is a splitting field of f_1 over $K(u)$ and that M is a splitting field of $\widetilde{\sigma} f_1$ over $L(u')$.

Now, applying the induction hypothesis, $\widetilde{\sigma}$ can be extended to an isomorphism from F to M. Hence σ is extendible to an isomorphism from F to M.

Now let S be arbitrary (i.e., S could be infinite). We consider triples (E, τ, E'), where $K \subset E \subset F$ and $L \subset E' \subset M$ and $\tau : E \to E'$ is an isomorphism such that $\tau\big|_K = \sigma$. Note that we don't have to worry about this "set" of triples T not being a set, since E and E' are just subsets of fields and τ is an isomorphism, so nothing strange could go on.

Partially order the triples by: $(E, \tau, E') \leq (E_1, \tau_1, E_1')$ if and only if $E \leq E_1$, $E' \leq E_1'$, and $\tau_1\big|_E = \tau$. Note that $T \neq \emptyset$ since $(K, \sigma, L) \in T$. To find an upper bound for any chain, we want to find an isomorphism $\alpha : \bigcup_{i \in I} E_i \to \bigcup_{i \in I} E_i'$. If $u \in \cup E_i$, then $u \in E_i$ for some i. Define $\alpha(u) = \tau_i(u)$.

To see that α is well defined: this does not depend on choice of E_i containing u, since if $u \in E_i \subset E_j$, then $\tau_j\big|_{E_i} = \tau_i$. So, the triple $(\cup E_i, \alpha, \cup E_i')$ is an upper bound for any chain over i. We have verified the hypothesis of Zorn's Lemma, so there exists some maximal element $(F_0, \tau_0, M_0) \in T$.

Claim: $F_0 = F$, and $M_0 = M$.

Proof: Suppose toward a contradiction that $F_0 \subsetneq F$. Then there exists a polynomial $f \in S$ such that f does not split over F_0. Let $u \in F \setminus F_0$ be a root of f. u' is a root in M of the corresponding factor of $\sigma f \in M_0[x]$.

$$\begin{array}{ccc} F & & M \\ \cup & & \cup \\ F_0(u) & \longrightarrow & M_0(u') \\ \cup & & \cup \\ F_0 & \xrightarrow{\tau_0} & M \\ \cup & & \cup \\ K & \xrightarrow{\sigma} & L \end{array}$$

By an earlier Theorem, τ_0 can be extended to an isomorphism $F_0(u) \to M_0(u')$. This contradicts the maximality of (F_0, τ_0, M_0). Hence $F = F_0$. Clearly, since F is a splitting field for S over K and $F = F_0$, we have that $\tau_0(F_0) \subseteq M$ is a splitting field for S' over L. Hence $\tau_0(F_0) = M$. □

Definition: An irreducible polynomial $f \in K[x]$ is separable if the roots of f in a splitting field are distinct. If $K \subset F$, then $u \in F$ is separable over K if it is algebraic over K and its corresponding irreducible polynomial in $K[x]$ is separable. A field extension $K \subset F$ is separable if every element of F is separable over K.

Remark: In a field with characteristic 0, every polynomial is separable. This is an exercise.

Example: Let $K = \mathbb{F}_2(t)$ (the field of rational functions in F_2) and let $f \in K[x]$ be $x^2 - t$. Clearly K does not contain any roots of f, so f is irreducible. But, if u is a root of f in some extension of K, say $K(u)$, then we have

$$f = x^2 - u^2 = (x + u)(x - u) = (x - u)^2.$$

Hence, f is an inseparable polynomial.

Theorem V.3.11: Let F be an extension of K. The following are equivalent:

(i) F is algebraic and Galois over K.

(ii) F is separable over K and F is a splitting field of a set S of polynomials in $K[x]$.

(iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

Proof of (1) $\implies$ [(2) & (3)]**:** Let $u \in F$. Let $f \in K[x]$ be the irreducible monic polynomial with $f(u) = 0$. Let $\{u = u_1, u_2, \ldots, u_k\}$ be the roots of f in F (since F is algebraic).Let $g(x) = (x - u_1) \cdots (x - u_k)$. Then, $\mathrm{Aut}_K F$ permutes the roots, so fixes $g(x)$.

Since F is Galois over K, we have that $g(x) \in K[x]$. So, $f \mid g$, but $\deg g \leq \deg f$, and thus $f = g$. Hence F splits over F and all the roots are distinct, so u is separable. Hence F is separable over K. □

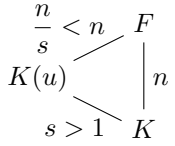
Proof of (2) $\implies$ (3)**:** From the set S let T be the subset of irreducible polynomials. Then F is a splitting field over K of T. □

Proof of (3) $\implies$ (1)**:** Since F is a splitting field of polynomials in K, it's algebraic over K. Let $u \in F \setminus K$. We have to find $\sigma \in \mathrm{Aut}_K F$ with $\sigma(u) \neq u$. Note that u is algebraic over K. $u \in K(u_1, \ldots, u_k)$, where u_i are roots of some elements of T (even if T is infinite, u can be written as a combination of a finite number of roots).

Let $E = K(u_1, \ldots, u_k, \ldots, u_t)$, where the u_i are now all roots of the irreducible monic polynomials of $\{u_1, \ldots, u_k\}$, i.e., E is the splitting field of a finite subset of T. Suppose there exists $\tau \in \mathrm{Aut}_K E$ such

that $\tau(u) \neq u$. Then, by one of our theorems on splitting fields, τ can be extended to $\sigma \in \operatorname{Aut}_K F$. So, it is sufficient to consider the finite case.

Assume $F = E$, i.e., T is finite. Then, $|F : K|$ is finite as well. We will argue by induction on $n := \big[F : K\big]$. Let $g \in K[x]$ be the minimal polynomial of u and let $s = \deg g$.



So, $\frac{n}{s} = |\operatorname{Aut}_{K(u)} F|$.

Let K_0 be the fixed field of $\operatorname{Aut}_K F$. Then, $K_0 \supset K$, and $\big[F : K_0\big] = |\operatorname{Aut}_K F|$, and F is Galois over K_0 (by **Artin**). So, in order to prove that $K = K_0$, we just have to show that $\big[F : K\big] = |\operatorname{Aut}_K F|$.

Let $H = \operatorname{Aut}_{K(u)} F =$ the stabilizer in $\operatorname{Aut}_K F$ of u. The function g has s distinct roots in F. If u_i is any root of g, then $K(u) \cong K(u_i)$, and this isomorphism can be extended to a K-isomorphism of F (by a **Theorem** on splitting fields), i.e., $\operatorname{Aut}_K F$ acts transitively on the set of s roots of g. Hence, $\big[\operatorname{Aut}_K F : H\big] = s$ by the **Orbit-Stabilizer Theorem**. So, $|\operatorname{Aut}_{K(u)} F| = \frac{n}{s}$ and $\big[\operatorname{Aut}_K F : H\big] = s$. Hence $|\operatorname{Aut}_K F| = n$ and so $K = K_0$. $\square$

Definition: We say that an extension $K \subset F$ is a normal extension if every polynomial in $K[x]$ which has a root in F, actually splits in F.

Theorem V.3.14: Let F be an algebraic extension of K. The following are equivalent:

(i) F is normal over K.

(ii) F is a splitting field of some set of polynomials in $K[x]$.

(iii) If $\overline{K}$ is an algebraic closure of K containing F, then for any K-monomorphism $\sigma : F \to \overline{K}$, we have $\sigma(F) = F$.

Special Topic: Two Applications

Theorem V.3.16: Suppose E is an algebraic extension of K. Then, there exists an extension $F \supset E$ called the normal closure of K such that

(1) F is normal (and algebraic) over K.

(2) No proper subfield of F containing E is normal over K.

(3) If E is separable over K, then F is Galois over K.

(4) If E is finite dimensional over K, then F is finite dimensional over K.

Proof: E contains some of the roots of some polynomials in K, so we let F contain all of the roots of those polynomials. This gives us that F is a splitting field over K and hence normal, hence (1). A proper subfield of F is missing some roots of polynomials, and hence is not normal over K, hence (2). If E is separable, then each polynomial that has roots in E is separable. So, F is Galois by **Theorem 3.11**, hence (3). If E is finite dimensional extension, then it adjoins a finite number of roots from K, hence the roots from a finite number of polynomials. Hence F is finite dimensional over K, hence (4).

Primitive Element Theorem (V.6.15): Let $K \subset F$ be a finite dimensional field extension. Assume either (1) [K is finite], or (2) [K is infinite and F is a separable extension of K]. Then, there exists $u \in F$ such that $F = K(u)$.

Proof: We proved case (1) in 5000 algebra: If K is a finite field, then F as a finite dimensional extension is also a finite field, and so its multiplicative group $F^\times$ is cyclic. Pick u to be a generator of that multiplicative group, and then $F = K(u)$ is clear.

Note in case (2) that every field of characteristic zero is a separable extension, so this theorem applies to it. Let F be a finite dimensional separable extension over K, and let E be the normal closure of K. Hence E is Galois over K by **Theorem V.3.16**. Thus, there exists finitely many intermediate fields $K \subset M \subset E$. So, there are only finitely many intermediate fields $K \subset M \subset F$.

If $F = K$, we're done vacuously. Otherwise $F \supsetneq K$, and we can choose $u \in F$ such that $|K(u) : K|$ is maximal. We will now show that $K(u) = F$.

Suppose $K(u) \neq F$. Then, there exists $v \in F \setminus K(u)$. Consider the set $\{K(u + av) \mid a \in K\}$. By finiteness of this set (by the finite number of intermediate fields) and infiniteness of K , there exist $a, b \in K$ such that $a \neq b$ and $K(u + av) = K(u + bv) =: L$.

So, since $u + av \in L$ and $u + bv \in L$, then the difference $(a - b)v \in L$, hence $v \in L$ and so $u \in L$. Hence $K(u + av) = L \supset K(u, v) \supsetneq K$. Since $K(u + av)$ is a simple extension, this contradicts the maximality by degree of $K(u)$. So, $K(u) = F$. $\square$

Special Topic: The Fundamental Theorem of Algebra

Fundamental Theorem of Algebra: $\mathbb{C}$ is algebraically closed.

Remark: We assume that:

(A) Every element of $\mathbb{C}$ has a square root.

(B) Every real polynomial of odd degree has a real root.

Proof: We show that there is no nontrivial finite extension of $\mathbb{C}$. Suppose F is a finite extension of $\mathbb{C}$. Then F is a finite extension of $\mathbb{R}$, and of course F is separable over $\mathbb{R}$.

Let E be the normal closure of F over $\mathbb{R}$. So, E is a finite Galois extension of $\mathbb{R}$. By the **Fundamental Theorem of Galois Theory**, the subgroups of $\operatorname{Aut}_{\mathbb{R}} F$ are in bijection with the intermediate fields $\mathbb{R} \subset M \subset E$. Note that $|\operatorname{Aut}_{\mathbb{R}} E| < \infty$.

Let H be a Sylow 2-subgroup of $\operatorname{Aut}_{\mathbb{R}} E$. Then, $|\operatorname{Aut}_{\mathbb{R}} E : H|$ is odd, and $|\operatorname{Aut}_{\mathbb{R}} E : H| = |H' : \mathbb{R}|$. Suppose that $u \in H' \setminus \mathbb{R}$. Then, $|\mathbb{R}(u) : R| \mid |H' : \mathbb{R}|$, and so is odd. Therefore, an irreducible polynomial of u over $\mathbb{R}$ has odd degree, which contradicts assumption (B). Thus, $H' = \mathbb{R}$, and so $H = \operatorname{Aut}_{\mathbb{R}} E$ (since $H'' = \mathbb{R}'$) and therefore H is a 2-group.

Then, since $\operatorname{Aut}_{\mathbb{C}} E \leq \operatorname{Aut}_{\mathbb{R}} E$, we have that $|\operatorname{Aut}_{\mathbb{C}} E| = 2^m$ for some $m \geq 0$. We prove that $m = 0$, and hence $E = \mathbb{C}$ and thus $F = \mathbb{C}$. Suppose $m \geq 1$. Then, $\operatorname{Aut}_{\mathbb{C}} E$ has a subgroup J of index 2. Then, $|J' : \mathbb{C}| = 2$. Then, for $u \in J' \setminus \mathbb{C}$, the irreducible polynomial in $\mathbb{C}[x]$ is of degree 2. But, by assumption (A) and the quadratic formula, every polynomial of degree 2 in $\mathbb{C}[x]$ splits over $\mathbb{C}$. This is a contradiction and thus $m = 0$, so $F = \mathbb{C}$.

So, the only finite extension of $\mathbb{C}$ is the trivial one, hence $\mathbb{C}$ is algebraically closed. $\square$

1.1.4 Section V.4 - The Galois Group of a Polynomial

Definition: Let $f(x) \in K[x]$. Then, the Galois group of $f(x)$ is $\mathrm{Aut}_K F$, where F is a splitting field of $f(x)$ over K. Note that Hungerford uses the term Galois group to refer to any such group. Other books sometimes only refer to a Galois group only if it is such a group of a Galois extension.

Remark: A finite extension of a finite field is automatically separable. Let $F \supset K$ with $|F| = q$. Consider $x^q - x \in K[x]$. Every element of F is a root of this polynomial. So, this polynomial has exactly q roots in F, and these roots must be distinct, hence all irreducible factors of this polynomial have distinct roots, thus it's separable. So, every element of F is separable. Thus F is separable.

Theorem V.4.2: Let $f \in K[x]$, with Galois group G.

(i) G is isomorphic to a subgroup of some symmetric group S_n.

(ii) If f is irreducible and separable of degree n, then G is isomorphic to a transitive subgroup of S_n, with n such that $n \mid |G|$.

Recall: We have a separable polynomial $f \in K[x]$ of degree n, with splitting field F. Let, F is Galois over K, and $F = K(u_1, \ldots, u_n)$ for u_i the distinct roots of f in F. $\mathrm{Aut}_K F$ acts on $\{u_1, \ldots, u_n\}$, giving an injective homomorphism $\mathrm{Aut}_K F \hookrightarrow S_n$. The action of $\mathrm{Aut}_K F$ on $\{u_1, \ldots, u_n\}$ is *transitive*. So, we can identity $\mathrm{Aut}_K F$ with a certain transitive subgroup of S_n.

Example: (Degree 2) Let K be a field, $f \in K[x]$ a separable polynomial with degree 2, with Galois group G. Then, $G \cong Z_2$. This is trivial in the same sense that the "quadratic formula" is easy and well-known to everybody.

Definition: Suppose that $\mathrm{char}\, K \neq 2$, $f \in K[x]$ of degree n with n distinct roots $u_1, \ldots, u_n$, in a splitting field. Define

$$\Delta := \prod_{i<j} (u_i - u_j).$$

Then, $D = \Delta^2$ is called the discriminant of f.

Proposition V.4.5:

(1) $D \in K$,

(2) For $\sigma \in \mathrm{Aut}_K F \leq S_n$, we have that

$$\sigma(\Delta) = \begin{cases} -\Delta, & \text{if } \sigma \text{ is odd} \\ \Delta, & \text{if } \sigma \text{ is even} \end{cases}$$

Corollary V.4.6: If D is a square in K, then $\mathrm{Aut}_K F \leq A_n$.

Corollary V.4.7: (Degree 3) Let K be a field with char $\neq 2, 3$. Let f be an irreducible separable polynomial of degree 3. The Galois group of f is either S_3 or A_3. It is A_3 if and only if the discriminant is a square in K.

Proposition V.4.8: Let $f(x) := x^3 + bx^2 + cx + d$, let $g(x) := f(x - \frac{b}{3})$. Then, $g(x)$ has the form $x^3 + px + q$, and the discriminant of f is $-4p^3 - 27q^2$.

Proof: (Sketch) $\Delta = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3)$. Do Δ^2 to get a symmetric polynomial, write in terms of the elementary symmetric polynomials (following the algorithm created by the proof that every symmetric polynomial can be written in terms of the elementary symmetric polynomials). Then we know that $u_1 + u_2 + u_3$ is the coefficient of x^2 so equals 0, and $u_1u_2 + u_1u_3 + u_2u_3$ is the coefficient of x so equals p and $u_1u_2u_3 = -q$. $\square$

Example: Consider $x^3 - 3x + 1 \in \mathbb{Q}[x]$. Then, $D = (-4)(-27) - 27 = 3(27) = 81 = 9^2$. So, the Galois group of this polynomial is A_3.

Example: Consider $f(x) = x^3 + 3x^2 - x - 1 \in \mathbb{Q}[x]$. Let $g(x) := f(x - \frac{b}{3}) = f(x - 1) = x^3 - 4x + 2$, which is irreducible by Eisenstein. Then, $D = 148$, which isn't a square, so the Galois group is S_3. In the cubic case, $D > 0$ if and only if $f(x)$ has three real roots.

Example: (Degree 4) Consider the group S_4 with normal subgroup $V_4 := \{1, (12)(34), (13)(24), (14)(23)\}$. How can we find an expression that is fixed by all of these things? Well, $\alpha := u_1u_2 + u_3u_4$ is fixed by the element $(12)(34)$ and actually by all four elements of V_4. Similarly $\beta := u_1u_3 + u_2u_4$ and $\gamma := u_1u_4 + u_2u_3$ are all fixed by all elements in V_4.

$$\begin{array}{ccc} \mathrm{Aut}_K F & \leq & S_4 \\ \triangledown & & \triangledown \\ V_4 \cap \mathrm{Aut}_K F & \leq & V_4 \end{array}$$

Lemma V.4.9: Under the Galois correspondence, $K(\alpha, \beta, \gamma)$ corresponds to $V_4 \cap \mathrm{Aut}_K F$. Hence $K(\alpha, \beta, \gamma)$ is Galois over K and $\mathrm{Aut}_K K(\alpha, \beta, \gamma) \cong \mathrm{Aut}_K(F/(\mathrm{Aut}_K F \cap V_4))$.

Proof: (Sketch) It's clear that $\mathrm{Aut}_K F \cap V_4$ fixes α, β, γ. It remains to show that if $\sigma \notin \mathrm{Aut}_K F$, then σ moves α, β, or γ.

By the second isomorphism theorem:

$$\mathrm{Aut}_K F/(\mathrm{Aut}_K F \cap V) \cong (\mathrm{Aut}_K F \cdot V)/V \leq S_4/V_4, \text{ which has order 6.}$$

Now you have to check manually all coset representatives of V_4 inside of S_4, and show that each moves α, β, or γ. Then you make α, β, γ into some cubic with splitting field $K(\alpha, \beta, \gamma)$, you can analyze that with the cubic method earlier. You get either a group of 2 or 4, and consider all transitive subgroups of S_4. $\square$

Remark: Let $\mathrm{char}(K) \neq 2, 3$, and $f(x) \in K[x]$ irreducible, separable, and of degree 4. Let F be splitting field, with u_1, u_2, u_3, u_4 the roots of $f(x)$ in F. Let $\alpha = u_1u_2 + u_3u_4$, let $\beta = u_1u_3 + u_2u_4$, and let $\gamma = u_1u_4 + u_2u_3$. We have the resolvant cubic: $(x - \alpha)(x - \beta)(x - \gamma)$. Now, $K(\alpha, \beta, \gamma) \longleftrightarrow G \cap V_4$, for $G = \mathrm{Aut}_K F \leq S_4$. We have the following diagram

$$\begin{array}{ccc} F & \longleftrightarrow & 1 \\ | & & | \\ K(\alpha, \beta, \gamma) & \longleftrightarrow & G \cap V_4 \\ | & & \triangle \\ K & \longleftrightarrow & G \end{array}$$

Now $\mathrm{Aut}_K(K(\alpha, \beta, \gamma)) \cong G/(G \cap V_4)$.

Lemma V.4.10: The resolvant cubic belongs to $K[x]$. If $f(x) = x^4 + bx^3 + cx^2 + dx + e$, then the resolvant cubic is

$$x^3 - cx^2 + (bd - 4e)x - (b^2e + 4ce - d).$$

Computing the Galois Group of Quartics:

G is a transitive subgroup of S_4, so has order divisible by 4. The possibilities are:

(-) S_4

(-) A_4

(-) V_4

(-) $D_8 \in \mathrm{Syl}_2(S_4)$ (there are three of these)

(-) Z_4, generated by a 4-cycle (there are three of these)

Proposition V.4.11: Let $m = |K(\alpha, \beta, \gamma) : K|$. Then,

$$\begin{aligned} m = 6 &\iff G = S_4, \\ m = 3 &\iff G = A_4, \\ m = 1 &\iff G = V_4, \\ m = 2 &\iff G = D_4 \text{ or } Z_4. \end{aligned}$$

In the last case $G \cong D_4$ if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong Z_4$ otherwise.

Proof: Note that $m = |\operatorname{Aut}_K(K(\alpha, \beta, \gamma))| = |G/(G \cap V_4)|$. If $G = S_4$, then of course by index orders, $m = 6$. Similarly, if $G = A_4$ then $m = 3$, and if $G = V_4$ then $m = 1$, and if $G = D_4$ or Z_4, then $m = 2$.

It remains to show the last statement. Let F be a splitting field for f over $K(\alpha, \beta, \gamma)$. Then,

$$\begin{aligned} f \text{ is irreducible in } K(\alpha, \beta, \gamma) &\iff \operatorname{Aut}_{K(\alpha,\beta,\gamma)} F = G \cap V \text{ acts transitively on the set of roots of } F. \\ &\iff G \cap V = V, \text{ since no proper subgroup of } V \text{ acts transitively.} \end{aligned}$$

So, f is irreducible in $K(\alpha, \beta, \gamma)$ if and only if $V \subseteq G$. $\square$

Example: Let $f(x) = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$. f is irreducible by Eisenstein's Criterion. Now, we find the resolvant cubic to be:

$$x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8).$$

So, $\alpha = 4$, $\beta = \sqrt{8}$, and $\gamma = \sqrt{8}$. Hence, $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2})$. Since $|\mathbb{Q}(\sqrt{2}) : \mathbb{Q}| = 2$, we have $m = 2$. Hence the Galois group is either D_4 or Z_4.

Consider $f(x)$ as an element of $\mathbb{Q}(\sqrt{2})$. Set $z := x^2$. Then, $f(z) = z^2 + 4z + 2$, and by the quadratic formula, $z = -2 \pm \sqrt{2}$. So, $f(x) = (x^2 + (2 + \sqrt{2}))(x^2 + (2 - \sqrt{2})) \in \mathbb{Q}(\sqrt{2})$. Hence f is not irreducible, and so $G = Z_4$.

Example: Let $f(x) = x^4 - 10x^2 + 4 \in \mathbb{Q}[x]$. f is irreducible, but we do not check that here. The resolvant cubic is:

$$x^3 + 10x^2 - 16x - 160 = (x + 10)(x + 4)(x - 4).$$

So, $\alpha, \beta, \gamma \in \mathbb{Q}$, thus $m = 1$ and so $G \cong V_4$.

Example: Let $f(x) = x^4 - 2$. f is irreducible by Eisenstein's Criterion. The resolvant cubic is:

$$x^3 + 8x = x(x + 2\sqrt{2}i)(x - 2\sqrt{2}i).$$

Now, $\alpha = 0$, $\beta = -2\sqrt{2}i$, and $\gamma = 2\sqrt{2}i$. So, $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\sqrt{2}i)$. Hence $m = 2$.

Now to determine if the Galois group is Z_4 or D_4. Let $F = \mathbb{Q}(\sqrt[4]{2}, i)$ be the splitting field of F. Then, since $\big[F : \mathbb{Q}\big] = 8$ and $\big[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}\big] = 2$, we must have that $\big[F : \mathbb{Q}(\sqrt{2}i)\big] = 4$. Since this extension has degree 4, we have the D_4 case. (In the Z_4 case, it would be 2.)

Theorem V.4.12: If p is a prime and $f(x) \in \mathbb{Q}[x]$ is irreducible of degree p and has precisely two non-real roots, then the Galois group of f is S_p.

Proof: Note that $S_p = \langle (1\ \ 2),\ (1\ \ 2\ \ \cdots\ \ p) \rangle$. See book for rest.

Example: Consider $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Sketch the graph to see that f has three real roots and hence two complex roots. f is irreducible by Eisenstein. Hence the Galois group of f is S_5.

1.1.5 Section V.5 - Finite Fields

Recall: Let R be a commutative ring with 1. Define

$$f(x) := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x].$$

Define the (formal) derivative to be

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

The product rule holds:

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

We now prove a lemma from earlier in the book:

Lemma III.6.10: Let E be an integral domain, D a subdomain (also an integral domain). Let $f(x) \in D[x]$ and $c \in E$. Then,

(i) c is a multiple root of $f(x)$ if and only if $f(c) = 0$ and $f'(c) = 0$.

(ii) If D is a field and f and f' are coprime, then f does not have multiple roots in E.

(iii) If D is a field and f is irreducible and E contains a root of f, then f has no multiple roots if and only if $f' \neq 0$.

Proof of (i): If c is a multiple root of $f(x)$, then

$$f(x) = (x-c)^m g(x), \text{ for } m > 1.$$

So,

$$f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x).$$

Hence $(x-c) \mid f'(x)$, so $f'(c) = 0$.

Conversely, if c is not a multiple root of $f(x)$, then the derivative would not have a factor of $(x-c)$. □

Proof of (ii): Suppose D is a field and f, f' are coprime. Then, there exists $A(x), B(x) \in D[x]$ such that $Af + Bf' = 1$. If there were a multiple root c in any extension field of D, then

$$1 = (Af + Bf')(c) = A(c)f(c) + B(c)f'(c) = A(c)(0) + B(c)(0) = 0,$$

which is a contradiction. □

Proof of (iii): If f is irreducible and $f' \neq 0$, then f and f' are coprime. So, f has no multiple roots in E. Conversely, if f has a root $b \in E$ and f has no multiple roots, then

$$f(x) = (x-b)g(x),$$

where $(x-b) \nmid g(x)$ and so $g(b) \neq 0$. Now,

$$f'(x) = g(x) + (x-b)g'(x).$$

Hence $f'(b) = g(b) \neq 0$. So $f' \neq 0$. □

Remark: In a finite field, the characteristic is p for some non-zero prime p, and the prime subfield is $\mathbb{F}_p$. Now, the whole finite field will be a vector space over $\mathbb{F}_p$ and thus is isomorphic to the direct product of some number of copies of $\mathbb{F}_p$. Hence $|F| = p^n$, where $n = \big[F : \mathbb{F}_p\big]$.

Proposition V.5.6: F is a finite field with p^n elements if and only if F is a splitting field of a polynomial $x^{p^n} - x \in \mathbb{F}_p[x]$.

Proof:
($\Longrightarrow$): Let E be a splitting field of $x^{p^n} - x$ over F. So, $E \supseteq F$. We want to show that $E = F$. Note that $|F^\times| = p^n - 1$. Hence, every non-zero $u \in F$ satisfies $u^{p^n-1} = 1$, by Lagrange. Hence, every (even zero) element $u \in F$ satisfies $u^{p^n} = u$. So, every element of F is a root of $x^{p^n} - x$. Hence $E \subseteq F$, and thus $E = F$. $\square$

($\Longleftarrow$): Note that $(x^{p^n} - x)' = -1 \neq 0$, so this polynomial has p^n distinct roots in a splitting field. It is not hard to verify that the set E of all roots of f in F is a subfield of F of order p^n. Hence, it contains the prime subfield $\mathbb{F}_p$ of F. Since F is a splitting field, it is generated over $\mathbb{F}_p$ by the roots of f (i.e., the elements of E). Thus, $F = \mathbb{F}_p(E) = E$. $\square$

Corollary: Every finite field is Galois over its prime subfield. (This is true because it is a splitting field of a set of separable irreducible polynomials.

Corollary V.5.7: Any two finite fields with the same number of elements are isomorphic.

Corollary V.5.9:

(a) For any n, there exists a field of order p^n.

(b) For any n, there exists an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.

Proof of (a): Take the splitting field of $x^{p^n} - x$. $\square$

Proof of (b): Let F be a field of order p^n. Then, $F^\times$ is cyclic. Let u be a generator of $F^\times$. Then $F = \mathbb{F}_p(u)$. So, the irreducible polynomial of u in $\mathbb{F}_p[x]$ has degree n. $\square$

Remark: Suppose $|F| = p^n$. Consider the map $\varphi : F \to F$ defined by $\varphi(u) = u^p$.
Then, $1 \mapsto 1^p = 1$, $uv \mapsto (uv)^p = u^p v^p$, and $u + v \mapsto (u + v)^p = u^p + v^p$ (because we have characteristic p).
Now, φ is a field monomorphism, and it's surjective since F is finite, so $\varphi \in \mathrm{Aut}(F)$.

Proposition V.5.10: Let $|F| = p^n$. Then, $\mathrm{Aut}_{\mathbb{F}_p} F = \langle\varphi\rangle$ is cyclic of order n.

Proof: Since F is Galois over $\mathbb{F}_p$ of degree n, it suffices to show that φ has order n. Suppose that $\varphi^m = \mathrm{Id}$. Then, $u^{p^m} = u$, for all $u \in F$. Hence, every element of F is a root of $f(x) := x^{p^m} - x$. Therefore, $p^m \geq |F| = p^n$, so $m \geq n$. On the other hand, we know that $u^{p^n} - u = 0$ for all $u \in F$. So, $\varphi^n = 1$. Thus $m = n$. $\square$

Remark: Given the following diagram, we must have that $s \mid r$:

$$\begin{array}{l} F \quad \text{order } p^r \\ \mid r/s \\ K \quad \text{order } p^s \\ \mid s \\ \mathbb{F}_p \end{array}$$

Now if $\mathrm{Aut}_{\mathbb{F}_p}(F) = \langle\varphi\rangle$, then $\mathrm{Aut}_K(F) = \langle\varphi^s\rangle$, by the Galois Correspondence. Additionally, $\mathrm{Aut}_{\mathbb{F}_p}(K) = \langle\varphi + \langle\varphi^s\rangle\rangle$.

1.1.6 Section V.6 - Separability

Definition: Let F be an extension of K. We say that $u \in F$ is purely inseparable over K if its irreducible polynomial $f(x)$ over K factors over F as $f(x) = (x-u)^m$.

Example: Consider $K = \mathbb{F}_p(x)$. In $K[t]$, consider $f(x) := t^p - x$. If u is a root of $f(x)$ in some splitting field, then $f(x) = (t-u)^p$.

Theorem V.6.2: Let F be an extension of K. Then $u \in F$ is both separable and purely inseparable over K if and only if $u \in K$.

Lemma V.6.3: Let F be an extension of K, with $\operatorname{char} K = p > 0$. If $u \in F$ is algebraic over K, then there exists $k \geq 0$ such that u^{p^k} is separable over K.

Proof: (by induction on the degree n of u over K) If $n = 1$, then $u \in K$, and so $u^{p^0} = u$, and we're done. We can assume that u is inseparable (if it's separable, we're done). So, if $f \in K[x]$ is the minimal polynomial of u, then $f' = 0$. So, $f(x) = g(x^p)$, for some $g \in K[x]$.

Hence u^p is a root of $g(x)$, and so has lower degree than u. By induction, there exists m such that $(u^p)^{p^m} = u^{p^{m+1}}$ is separable. $\square$

Theorem V.6.4: Let F be an algebraic extension of K, with $\operatorname{char} K = p > 0$. The following are equivalent:

(i) F is purely inseparable over K.

(ii) The irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$.

(iii) If $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$.

(iv) The only elements of F which are separable over K are the elements of K itself.

(v) F is generated over K by a set of purely inseparable elements.

Proof:

(i) $\Longrightarrow$ (ii):

Let $u \in F$. By (i), u is purely inseparable over K, with minimal polynomial $f(x) = (x-u)^m$, for $m \geq 1$. Let $m = p^r \cdot k$, where $p \nmid k$. Then, $f(x) = (x-u)^{p^r \cdot k} = ((x-u)^{p^r})^k = (x^{p^r} - u^{p^r})^k \in K[x]$. Expanding using the binomial theorem, the coefficient of $x^{p^r \cdot (k-1)}$ equals $\pm k u^{p^r} \in K$.

But, since $k^{-1} \in K$, we have that $u^{p^r} \in K$. Thus, $x^{p^r} - u^{p^r} \in K[x]$, and so $k = 1$ and $f(x) = x^{p^r} - u^{p^r}$. $\square$

(ii) $\Longrightarrow$ (iii):

Trivial, since if u satisfies $x^{p^n} - a$, then $u^{p^n} \in K$. $\square$

(i) $\Longrightarrow$ (iv):

Trivial, by the earlier Theorem. $\square$

(i) $\Longrightarrow$ (v):

Trivial, since if F purely inseparable over K, then every element in F is purely inseparable, and clearly F is generated by the set of all its own elements over K. $\square$

(iii) $\Longrightarrow$ (i):

If $u \in F$, then by assumption $u^{p^n} \in K$ for some $n \geq 0$. Now, u is a root of $x^{p^n} - u^{p^n} = (x-u)^{p^n} \in K[x]$, and so u is purely inseparable over K. $\square$

(iv) $\Longrightarrow$ (iii):

By assumption, the only elements that are separable over K are the elements of K. By the earlier Lemma that if $u \in F$ is algebraic then u^{p^n} is separable over K, we have that $u^{p^n} \in K$. $\square$

(v) $\Longrightarrow$ (iii):

If u is purely inseparable over K, then the proof of (i) $\Rightarrow$ (ii) shows that $u^{p^n} \in K$ for some $n \geq 0$. If $u \in F$ is arbitrary, use **Theorem 1.3** and the Freshman's Dream. $\square$

Corollary V.6.5: If F is a finite purely inseparable extension of K, then $\big[F : K\big] = p^n$ for some $n \geq 0$.

Lemma V.6.6: If F is an extension field of K, and $X \subseteq F$ such that $F = K(X)$, and every element of X is separable over K, then F is a separable extension over K.

Proof: We proved an equivalent statement when working with Galois extensions. Given F and K, we look at the splitting field containing all roots of all minimal polynomials of all elements in K, call this E, and now, $E \supset F \supset K$, and E is Galois over F, so E is separable. Now, every subfield of E is separable over K, so F is separable over K. $\square$

Main Theorem on Inseparability: Let F be an algebraic extension field of K, let S be the set of all elements of F which are separable over K, and P the set of all elements of F which are purely inseparable over K. Then,

(i) S is a separable extension field of K.

(ii) F is purely inseparable over S.

(iii) P is a purely inseparable extension field of K.

(iv) $P \cap S = K$.

(v) F is separable over P if and only $F = SP$.

(vi) If F is normal over K, then S is Galois over K, F is Galois over P and $\mathrm{Aut}_K\, S \cong \mathrm{Aut}_P\, F = \mathrm{Aut}_K\, F$.

1.1.7 Section V.7 - Cyclic Extensions

Lemma V.7.5: (Linear Independence of Field Automorphisms) Let $\sigma_1, \ldots, \sigma_n$ be distinct field automorphisms of F. Suppose there exists $a_1, \ldots, a_n \in F$ such that for all $u \in F$,

$$a_1\sigma_1(u) + \cdots + a_n\sigma_n(u) = 0.$$

Then, $a_i = 0$, for all i.

Proof: Suppose not. Among all possible relations of this type, choose a "shortest" one (i.e., with smallest number of non-zero coefficients). Without loss of generality, $a_1\sigma_1(u) + \cdots + a_k\sigma_k(u) = 0$ ($\bigstar$), for all $u \in F$, with $a_i \neq 0$ for $i \in [0 \,..\, k]$. Clearly, $k \geq 2$. Since $\sigma_1 \neq \sigma_2$, we can pick $v \in F$ such that $\sigma_1(v) \neq \sigma_2(v)$. Now, we can apply ($\bigstar$) to the element uv, to get

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_2(v) + \cdots + a_k\sigma_k(u)\sigma_k(v) = 0.$$

Multiplying ($\bigstar$) by $\sigma_1(v)$, we get

$$a_1\sigma_1(u)\sigma_1(v) + a_2\sigma_2(u)\sigma_1(v) + \cdots + a_k\sigma_k(u)\sigma_1(v) = 0.$$

Subtracting the second equation from the first:

$$a_2\sigma_2(u)[\sigma_2(v) - \sigma_1(v)] + \cdots + a_3\sigma_3(u)[\sigma_3(v) - \sigma_1(v)] + \cdots + a_k\sigma_k(u)[\sigma_k(v) - \sigma_1(v)] = 0.$$

By commutativity and associativity:

$$(a_2[\sigma_2(v) - \sigma_1(v)])\sigma_2(u) + \cdots + (a_3[\sigma_3(v) - \sigma_1(v)])\sigma_3(u) + \cdots + (a_k[\sigma_k(v) - \sigma_1(v)])\sigma_k(u) = 0$$

and we've arranged that $\sigma_2(v) - \sigma_1(v) \neq 0$. Hence, we now havt a "shorter" non-trivial relation that equals zero. This is a contradiction. Hence $a_i = 0$, for all i. $\square$

Definition: Let F be a finite Galois extension of K of degree n. For $u \in F$, define the trace and norm by

$$T_K^F(u) = T(u) := \sum_{\sigma \in \mathrm{Aut}_K F} \sigma(u),$$

$$N_K^F(u) = N(u) := \prod_{\sigma \in \mathrm{Aut}_K F} \sigma(u).$$

Note that for all $u \in F$, we have that $T_K^F(u) \in K$ and $N_K^F(u) \in K$. To see this, note that if you apply any automorphism to $T_K^F(u)$, it will permute the sum, and the sum stays the same, so $T_K^F(u)$ is fixed by all automorphisms, hence it's in K. Same argument for $N_K^F(u)$. Also note that T_K^F is a K-linear map from F to K.

Theorem V.7.6: Let F be a cyclic extension field of K of degree n, and let σ be a generator of $\mathrm{Aut}_K F$ and let $u \in F$. Then,

(a) $T_K^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$.

(b) $N_K^F(u) = 1_K$ if and only if $u = v\sigma(v)^{-1}$ for some nonzero $v \in F$. (Hilbert's Theorem 90)

Proof:
($\Longleftarrow$, (a)):

The ($\Longleftarrow$) direction is clear, since $T(v) = T(\sigma v)$ and $N(v) = N(\sigma v)$. $\square$

($\Longrightarrow$, (a)):

By linear independence of $\{1, \sigma, \ldots, \sigma^{n-1}\}$, there exists $z \in F$ such that $z+\sigma z+\cdots+\sigma^{n-1}z \neq 0$, i.e., $T(z) \neq 0$. Then, by K-linearity of T, there exists $w \in F$ such that $T(w) = 1$.

Suppose $T(u) = 0$. Define

$$v = uw + (u + \sigma u)(\sigma w) + (u + \sigma u + \sigma^2 u)(\sigma^2 w) + \cdots + (u + \sigma u + \cdots + \sigma^{n-2}u)(\sigma^{n-2}w).$$

Now,

$$\sigma v = \sigma u \sigma w + (\sigma u + \sigma^2 u)(\sigma^2 w) + \cdots + (\sigma u + \sigma^2 u + \cdots + \sigma^{n-1}u)(\sigma^{n-1}w).$$

Subtracting:

$$v - \sigma v = uw + u(\sigma w) + u(\sigma^2 w) + \cdots + u(\sigma^{n-1}w) = uT(w) = u1_K = u,$$

using the fact that $0 = T(u) = u + \sigma u + \cdots + \sigma^{n-1}u$ and so $u = -(\sigma u + \cdots + \sigma^{n-1}u)$. $\square$

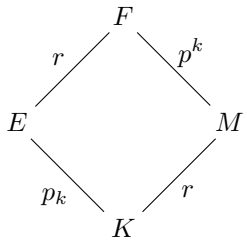
($\Longrightarrow$, (b)):

Suppse $N(u) = 1_K$, so $u \neq 0$. (Such a u exists since $N(1) = 1$.) By linear independence, there exists $y \in F$ such that $v \neq 0$, where

$$v = uy + (u\sigma u)\sigma y + (u\sigma u\sigma^2 u)\sigma^2 y + \cdots + (u\sigma u \cdots \sigma^{n-2}u)\sigma^{n-2}y + (u\sigma u \cdots \sigma^{n-1}u)\sigma^{n-1}y.$$

Since the last summand of v is $N(u)\sigma^{n-1}y = 1_K\sigma^{n-1}y = \sigma^{n-1}y$, we see that $u^{-1}v = \sigma v$, and therefore $y = v\sigma(v)^{-1}$ (which is okay since $\sigma(v) \neq 0$ since $v \neq 0$ and σ is injective). $\square$

Remark: Let $p := \operatorname{char} K$. Let n be the degree of F over K, with $n = p^k r$ and $p \nmid r$. We split the field F into separable and purely inseparable parts as last class, and have the following diagram.



We can analyze one of the r-extensions by using the trace and the other r-extension using the norm.

Remark: Let F be a cyclic extension field of K of degree n. **Proposition V.7.7** (see book) allows us to consider two cases: (i) $n := \operatorname{char}(K) = p \neq 0$, and (ii) either $\operatorname{char}(K) = 0$ or [$\operatorname{char}(K) = p \neq 0$ and $\gcd(n, p) = 1$]. The next proposition considers the first case.

Proposition V.7.8: Let K be a field of characteristic p. Then, F is a cyclic extension of degree p if and only if F is a splitting field over K of an irreducible polynomial of the form $x^p - x - a \in K[x]$. In this case, $F = K(u)$, where u is any root of $x^p - x - a$.

Proof:
($\Longrightarrow$):

Let σ be a generator of $\operatorname{Aut}_K F$. Then, $T(1_F) = p1_K = 0$. So, there exists $v \in F$ such that $1 = v - \sigma(v)$. Let $u = -v$. Then, $\sigma(u) = -\sigma(v) = 1 - v = 1 + u$. So $\sigma(u^p) = \sigma(u)^p = (1+u)^p = 1 + u^p$. Hence, $\sigma(u^p - u) = u^p - u$, and so $u^p - u \in K$. Let $a := u^p - u \in K$. Then, u is a root of $x^p - x - a \in K[x]$.

To show F is a splitting field of $x^p - x - a$, it suffices to show that F contains all p roots. Since $\sigma(u) = 1 + u$, we have that $\sigma^2(u) = u + 2$, etc. So, $\sigma^i(u) = u + i$, for all $i \in \mathbb{F}_p$, and all these

elements are distinct. Thus, the set $\{u+i \mid i \in \mathbb{F}_p\}$ is a set of p distinct roots of $x^p - x - a$. Hence $x^p - x - a$ splits in F.

Moreover, since all the roots are conjugate under $\mathrm{Aut}_K F$, it follows that $x^p - x - a$ is irreducible. (Otherwise, if it were irreducible, automorphisms could only move factors among irreducible factors.) $\square$

($\Longleftarrow$):

Conversely, suppose F is a splitting field for an irreducible polynomial $x^p - x - a$. Let u be a root. Then, $(u+i)^p - (u+i) = u^p + i^p - u - i = u^p - u = a$, since $i^p = i$. So, $\{u+i \mid i \in \mathbb{F}_p\}$ is the set of p distinct roots of $x^p - x - a$. Hence, $\big[F : K\big] = p$ and this polynomial has distinct roots in F, so F is Galois over K. Since the only group of order p is cyclic, we must have that F is a cyclic extension of K. $\square$.

Remark: To hande the second case, we need to introduce an additional hypothesis: We assume K contains a primitive n^{th} root of unity ζ, where $p \nmid n$. Consider $f(x) = x^n - 1 \in K[x]$. Then $f'(x) = nx^{n-1}$, and we see that $f(x)$ and $f'(x)$ are coprime. Thus $f(x)$ must have n distinct roots, namely $\{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$. The set $\{u \in \overline{F} \mid u^n = 1\}$ is a multiplicative subgroup of $\overline{F}^{\times}$ of order n, and hence cyclic. So, a primitive n^{th} root of 1 is equivalent to a generator in this cyclic group. (Recall we assumed that K in fact does contain at least one primitive n^{th} root.)

Lemma V.7.10: Let n be a positive integer, and let K be a field with a primitive n^{th} root of unity ζ. (This implies by the above discussion that K has characteristic p with $p \nmid n$.)

(i) If $d \mid n$, then $\zeta^{n/d}$ is a primitive d^{th} root of unity.

(ii) If $d \mid n$ and u is a nonzero root of $x^d - a \in K[x]$, then $x^d - a$ has d distinct roots, namely $\{u, \zeta^{n/d}u, \ldots, \zeta^{(n/d)(d-1)}u\}$. Also, $K(u)$ is a splitting field for $x^d - a$, and is Galois over K.

Theorem V.7.11: Let n be a positive integer and K a field containing a primitive n^{th} root of unity ζ. Then, the following conditions on an extension F of K are equivalent:

(i) F is cyclic of degree $d \mid n$.

(ii) F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$.

(iii) F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$, with $d \mid n$.

Proof:
(ii) $\Longrightarrow$ (i):

Let $u \in F$ be a root of $x^n - a$. Then, the other roots are $\{\zeta^i u \mid i \in \mathbb{F}_p\}$ and so F is Galois over K. Thus, $F = K(u)$ and any $\sigma \in \mathrm{Aut}_K F$ is completely determined by $\sigma(u)$.

Suppose $\sigma, \tau \in \mathrm{Aut}_K F$ and $\sigma(u) = \zeta^i u$ and $\tau(u) = \zeta^j u$. Then , $\sigma\tau(u) = \sigma(\zeta^j u) = \zeta^j \sigma(u) = \zeta^j \zeta^i u = \zeta^{i+j} u$. Hence, the assignment $\sigma \mapsto i$ if and only if $\sigma(u) = \zeta^i u$ is a homomorphism from $\mathrm{Aut}_K F$ to Z_n, which is injective. Hence, $\mathrm{Aut}_K F \cong$ some subgroup of Z_n, i.e., $\mathrm{Aut}_K F \cong Z_d$ for some $d \mid n$. $\square$

(i) $\Longrightarrow$ (iii)

By hypothesis, $\mathrm{Aut}_K F = \langle \sigma \rangle$, with $\sigma^d = 1$. Let $\eta := \zeta^{n/d}$ be a primitive d^{th} root of unity in K. Now, $N_K^F(\eta) = \eta^{|F:K|} = \eta^d = 1$. By **Hilbert's Theorem 90**, $\eta = w\sigma(w)^{-1}$, for some $w \in F$. Let $v = w^{-1}$. Then $\sigma(v) = \sigma(w)^{-1} = \eta w^{-1} = \eta v$. Mimic the proof when we had $u + i$ earlier, and we're done. (Compute $\sigma(v^d) = (\eta v)^d = \eta^d v^d = v^d$. So, $v^d =: b \in K$, and v is a root of $x^d - b \in K[x]$.) $\square$

1.1.8 Section V.8 - Cyclotomic Extensions

Lemma: (Follows from the division algorithm in Euclidean Domains) Let R be a commutative ring with 1, and let $f, g \in R[x]$. Assume that the leading coefficient of g is a unit in R. Then, there exists a unique $q, r \in R[x]$ such that $f = gq + r$, with $r = 0$ or $\deg(r) < \deg(g)$. (i.e., We can do the Euclidean Algorithm in an arbitrary commutative ring when g has a unit as its leading coefficient.)

The Lemma applies to $\mathbb{Z}[x]$. So, given $f, g \in \mathbb{Z}[x]$ such that g is monic, then there exists a unique $q, r \in \mathbb{Z}[x]$ such that $f = gq + r$, with $r = 0$ or $\deg(r) < \deg(g)$. By uniqueness, q and r must be the same as if we used the Euclidean algorithm over $\mathbb{Q}[x]$.

Corollary: If $f, g \in \mathbb{Z}[x]$ with g monic, and $f = gh$ in $\mathbb{Q}[x]$, then we must have $h \in \mathbb{Z}[x]$.

Definition: Let K be a field. A cyclotomic extension of K of order n is a splitting field of $x^n - 1 \in K[x]$.

Remark: If $n = p^r m$ with $p \nmid m$, and $\mathrm{char}(K) = p$, then the cyclotomic extensions of order m and order n are the same. So, we assume henceforth that $p \nmid n$.

Theorem V.8.1: Let n be a positive integer, and let $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p \nmid n$. Let F be a cyclotomic extension of K of order n. Then,

(i) $F = K(\zeta)$, where $\zeta \in F$ is a primitive n^{th} root of unity.

(ii) F is an abelian extension of degree d, for some $d \mid \varphi(n)$. If n is prime, then F is cyclic.

(iii) $\mathrm{Aut}_K F$ is isomorphic to a subgroup $(\mathbb{Z}/n\mathbb{Z})^\times$.

Hint: Prove (iii) before (ii), then use (iii) to prove (ii).

Definition: Let n be a positive integer. Let K be a field with characteristic 0 or characteristic $p \nmid n$. Let F be a cyclotomic extension of K of order N. The n^{th} cyclotomic polynomial over K is the monic polynomial $g_n(x) = (x - \zeta_1) \cdots (x - \zeta_r)$, where $\zeta_1, \ldots, \zeta_r$ are the distinct primitive n^{th} roots of unity in F. (So, $r = \varphi(n)$.)

Proposition V.8.2:

(i) $x^n - 1 = \prod_{d \mid n} g_d(x)$.

(ii) The coefficients of $g_n(x)$ lie in the prime subfield P of K. If $P = \mathbb{Q}$, then the coefficients are integers.

(iii) $\deg g_n = \varphi(n)$.

Remark: Use the formula $\sum_{d \mid n} \varphi(d) = n$.

Proof of (ii): (By induction on n, sketch.) The $n = 1$ case is trivial. Now assume true for all $k < n$ with $\gcd(k, p) = 1$. We can write

$$g_n(x) \cdot \prod_{\substack{d \mid n \\ d \neq n}} g_d(x) = x^n - 1.$$

The right hand side has coefficients in P, and the right term of the left hand product has coefficients in P by induction. Compare the Euclidean Algorithm in $K[x]$ and $P[x]$, and you will see that we must have $g_n(x) \in P[x]$. $\square$

Proposition V.8.3: Let F be a cyclotomic extension of order n of $\mathbb{Q}$ and $g_n(x)$ the n^{th} cyclotomic polynomial. Then,

(i) $g_n(x)$ is irreducible in $\mathbb{Q}[x]$.

(ii) $\big[F : \mathbb{Q}\big] = \varphi(n)$.

(iii) $\text{Aut}_{\mathbb{Q}} F \cong (Z/n\mathbb{Z})^{\times}$.

Proof of (i): By Gauss' Lemma, it suffices to prove that $g_n(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$. Suppose toward a contradiction that $g_n(x)$ does factor in $\mathbb{Z}[x]$. Let h be an irreducible factor of g_n in $\mathbb{Z}[x]$ with $\deg h \geq 1$, and let ζ be a root of h in F and write $g_n(x) = h(x)f(x)$, for $f(x) \in \mathbb{Z}[x]$ monic. To show that all roots of $g_n(x)$ are roots of $h(x)$, hence that $g_n(x)$ is irreducible, it suffices to show that for any prime p with $\gcd(p, n) = 1$, ζ^p is a root of $h(x)$. (The reason is because all roots of $g_n(x)$ are of the form ζ^m for some m with $(m, n) = 1$.)

Suppose ζ^p is not a root of h. Then, ζ^p is a root of f. Hence, ζ is a root of the polynomial $f(x^p) \in \mathbb{Z}[x]$. Thus, $h(x) \mid f(x^p)$ in $\mathbb{Q}[x]$. Suppose $f(x^p) = h(x)k(x)$. Since $f(x^p) \in \mathbb{Z}[x]$ and $h(x)$ is monic, we must have that $k(x) \in \mathbb{Z}[x]$.

Reducing modulo p, we have that $\overline{f}(x^p) = \overline{h}(x)\overline{k}(x)$. The operation of reducing modulo p is a ring homomorphism from $\mathbb{Z}[x]$ to $\mathbb{F}_p[x]$. By the freshman's dream, $\overline{f}(x^p) = \overline{f}(x)^p$. So, $\overline{h}(x) \mid \overline{f}(x)^p$, and hence some irreducible factor of $\overline{h}(x)$ of positive degree divides $\overline{f}(x)$. Since $g_n(x) \mid x^n - 1$, we have that $x^{n-1} = h_n(x)r(x) = f(x)h(x)r(x)$. So, in $\mathbb{F}_p[x]$, $x^n - \overline{1} = \overline{f}(x)\overline{h}(x)\overline{r}(x)$, but we just showed that $\overline{f}(x)$ and $\overline{h}(x)$ have a common factor. Thus $x^n - \overline{1}$ has multiple roots, which is a contradiction because $\gcd(n, p) = 1$. $\square$

1.1.9 Section V.9 - Radical Extensions

Definition: An extension field F of K is a radical extension if $F = K(u_1, \ldots, u_n)$, and some positive power of u_i lies in $K(u_1, \ldots, u_{i-1})$, for all $1 \leq i \leq n$.

Lemma V.9.3: If F is a radical extension of K and N is a normal closure of F over K, then N is a radical extension over K.

Proof: (See book, pg. 304.)

Definition: Let K be a field, and let $f \in K[x]$. We say that the equation $f(x) = 0$ is separable by radicals if there exists a radical extension F of K and a splitting field E of $f(x)$ with $K \subset E \subset F$.

Theorem V.9.4: Let F be a radical extension field of K, and E an intermediate field. Then, $\mathrm{Aut}_K E$ is a solvable group.

Proof: Let K_0 be the fixed field of $\mathrm{Aut}_K E$. Then, E is Galois over K_0, with Galois group $\mathrm{Aut}_{K_0} E = \mathrm{Aut}_K E$. So, without loss of generality, assume $K = K_0$, i.e., E is Galois over K. Let N be the normal closure of F. Since E is Galois over K, we have that E is stable under $\mathrm{Aut}_K N$. Now, we have a homomorphism $\varphi : \mathrm{Aut}_K N \to \mathrm{Aut}_K E$ by restriction, i.e., $\varphi : \sigma \mapsto \sigma\big|_E$. Also, since N is a splitting field (normal) over K, every $\tau \in \mathrm{Aut}_K E$ extends to N, i.e., φ is onto. Thus, $\mathrm{Aut}_K E$ is a homomorphic image of $\mathrm{Aut}_K N$. So it suffices to prove that $\mathrm{Aut}_K N$ is solvable.

We have by the **Lemma** above that N is a radical extension of K. It's also a normal extension of K. Let K_1 be the fixed field of $\mathrm{Aut}_K N$. Again, N is Galois over K_1 with Galois group $\mathrm{Aut}_{K_1} N = \mathrm{Aut}_K N$, so without loss of generality we can let $K = K_1$. Now, N is Galois, radical, and normal over K, and it remains to show that if E is a Galois, radical extension of K, then $\mathrm{Aut}_K E$ is solvable. (So we now change the name of N back to E, and we just prove this statement.)

Now, E is a Galois, radical extension of K, and we show that $\mathrm{Aut}_K E$ is solvable. So, $E = K(u_1, \ldots, u_m)$, with $u_i^{m_i} \in K(u_1, \ldots, u^{i-1})$. Suppose $\mathrm{char}\, K = p$, and write m_i as $p^r m_i'$, with $p \nmid m_i'$. Then, $u_i^{m_i} = (u_i^{m_i'})^{p^t}$, and hence $u_i^{m_i'}$ is purely inseparable over $K(u_1, \ldots, u_{i-1})$. However, since we know that E is Galois over K, all elements are separable over all intermediate fields. Hence $u_i^{m_i'}$ is separable and purely inseparable, and hence is in $K(u_1, \ldots, u_{i-1})$. So, without loss of generality, we can assume $m_i = m_i'$, i.e., the characteristic of the field does not divide the m_i. Let $m := m_1 m_2 \cdots m_n$, and let ζ be a primitive m^{th} root of unity (in some algebraic closure of E). Note that ζ exists since $p \nmid m$. We now have the diagram:

$$\begin{array}{ccc} E & \longrightarrow & E(\zeta) \\ \uparrow & & \uparrow \\ K & \longrightarrow & K(\zeta) \end{array}$$

$E(\zeta)$ is Galois over K and E is Galois over K, so $\mathrm{Aut}_K E \cong (\mathrm{Aut}_K E(\zeta))/(\mathrm{Aut}_E E(\zeta))$. Hence, it suffices to prove that $\mathrm{Aut}_K E(\zeta)$ is solvable, since quotients of solvable groups are solvable, so if $\mathrm{Aut}_K E(\zeta)$ is solvable, then so is $\mathrm{Aut}_K E$. We know that $K(\zeta)$ must be an abelian extension of K, and $\mathrm{Aut}_K K(\zeta) \cong (\mathrm{Aut}_K E(\zeta))/(\mathrm{Aut}_{K(\zeta)} E(\zeta))$, by the **Fundamental Theorem of Galois Theory**, and so $\mathrm{Aut}_{K(\zeta)} E(\zeta) \trianglelefteq \mathrm{Aut}_K E(\zeta)$. So, if $\mathrm{Aut}_{K(\zeta)} E(\zeta)$ is solvable, then so much be $\mathrm{Aut}_K E(\zeta)$ (since the quotient by it is abelian).

We are now reduced to the case where we can change notation and just have $\zeta \in K$ and $E = K(u_1, \ldots, u_n) \supset \cdots \supset K(u_1, u_2) \supset K(u_1) \supset K$, with each one of these being a cyclic extension over the other. Since these are Galois extensions, you look at their corresponding normal subgroups (by the **Fundamental Theorem** to get a chain of normal subgroups with quotients that must be cyclic. Hence, we're done. $\square$

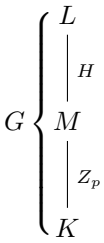
Corollary V.9.5: Let K be a field and $f \in K[x]$. If the equation $f(x) = 0$ is solvable by radicals, then the Galois group of f is a solvable group.

Notation: If F is an extension of K, then we use F/K to denote the extension of F over K, and we use $\mathrm{Gal}(F/K)$ to denote the Galois group of this extension.

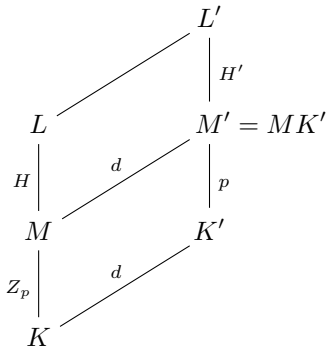
Theorem V.9.6: Let L/K be a finite Galois extension such that $G = \mathrm{Gal}(L/K)$ be solvable and $\mathrm{char}(K) \nmid \big[L : K\big]$. Then, there is a radical extension R/K such that $R \supset L \supset K$.

Proof: (by Strong Induction on $\big[L : K\big]$) The claim is obvious if $\big[L : K\big] = 1$, so assume that $\big[L : K\big] = n > 1$, and the theorem holds for all extensions of degree $< n$. Since $G \neq 1$ and G is solvable, there is $H \trianglelefteq G$ such that $\big[G : H\big] = p$ is prime. Let $\zeta_p \in K^{alg}$ be a primitive p^{th} root of unity. Such a ζ_p exists because $\mathrm{char}(K) \nmid |L : K|$, and so $\mathrm{char}(K) \neq p$.

Set $M = L^H$ (the fixed field of H in L, otherwise denoted H'). Now we have the diagram



Now set $K' := K(\zeta_p)$, $M' := M(\zeta_p)$, and $L' := L(\zeta_p)$. Since ζ_p is a root of $f(x) = \frac{x^p-1}{x-1}$, we have $\big[K' : K\big] \leq p - 1$. Hence $\big[K' : K\big]$ is prime to $\big[L : K\big]$.



Since $M' = MK'$, we have $\big[M' : K\big] \leq \big[M : K\big]\big[K' : K\big]$. We also have $\big[M : K\big] \mid \big[M' : K\big]$ and $\big[K' : K\big] \mid \big[M' : K\big]$. So, $\big[M' : K\big] = \big[M : K\big]\big[K' : K\big] = p\big[K' : K\big]$. Therefore $\big[M' : K\big] = p$. Since M/K is Galois, so is M'/K'. Hence $\mathrm{Gal}(M'/K') \cong Z_p$. Therefore, there exists $a \in K'$ such that $M' = K'(a^{1/p})$. "$a^{1/p}$" denotes any root of the equation $x^p - a$. (See **Kummer Theory** for explanation.) Hence $M' = K(\zeta_p, a^{1/p})$ is a radical extension of K.

Since L/M is Galois, so is L'/M'. Set $H' = \mathrm{Gal}(L'/M')$. (Shown on the diagram above.) Define $\varphi : H' \to H$ by $\varphi(\sigma) = \sigma\big|_L$. Then, φ is a well defined group homomorphism. If $\sigma \in \mathrm{Ker}\,\varphi$ then $\sigma\big|_L = \mathrm{Id}\big|_L$. Since $\sigma \in H'$, we have that $\sigma\big|_{M'} = \mathrm{Id}_{M'}$. Hence σ induces the identity on the composite field LM', and $LM' = L'$. Thus, σ is the identity on L' and so it was the identity to begin with. Hence $\mathrm{Ker}\,\varphi$ is trivial, and so φ is injective, and thus H' is isomorphic to a subgroup of H, and we know $H \leq G$. Since the subgroup of a solvable group is solvable, and G is solvable, so is H'. Using **Lagrange's Theorem**, we see that $\mathrm{char}(K) \nmid |H'|$. So, H' satisfies all hypotheses of the theorem. To use induction, we need to know that $|H'| < n$.

$|H'| = \big[L' : M'\big] < \big[L' : K'\big] \leq \big[L : K\big] = n$. Hence, by the induction hypothesis applied to L'/M', we have a radical extension R/M' such that $R \supset L' \supset M'$. Since M'/K is radical, we get that R/K is radical, and $R \supset L' \supset L \supset K$. So, we're done. $\square$

Corollary V.9.7: Let K be a field and let $f(x) \in K[x]$ with $\deg f = n \geq 1$. Then, assume that $\mathrm{char}(K) \nmid n!$ (i.e., $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$.) Then, $f(x) = 0$ can be solved with radicals if and only if the Galois group of $f(x)$ is solvable.

Proof: By the hypotheses, either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$, and so any irreducible factor of $f(x)$ is separable. Hence, the splitting field L of $f(x)$ over K is Galois over K. We've already proved that if $f(x) = 0$ is solvable by radicals, then $G = \mathrm{Gal}(L/K)$ is solvable.

Conversely, if G is solvable, we note that G acts faithfully on the roots of $f(x)$ (i.e., there is a homomorphism from G onto the roots of $f(x)$ which is injective). Hence, G is isomorphic to a subgroup of S_n. So, $|G| = \big[L : K\big] \mid n!$ (and so by assumption $\mathrm{char}(K) \nmid \big[L : K\big]$. By the theorem above, we get that there is a radical extension L of this splitting field and so that polynomial $f(x) = 0$ can be solved by radicals. $\square$

Example: Let $\mathrm{char}(K) \neq 2, 3$, and let $f(x) \in K[x]$, with $1 \leq \deg f \leq 4$. Then, $f(x) = 0$ can be solved by radicals. This is because the Galois group of the splitting field of a polynomial with degree at most 4 must be a subgroup of S_4, which is solvable.

Example: Let $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein. It follows from this and that 5 is prime that the Galois group has a 5-cycle and a 2-cycle (the complex conjugation between the two complex roots), and any subgroup of S_5 containing a 5-cycle and a 2-cycle is all of S_5, which is not solvable, and so $f(x) = 0$ cannot be solved with radicals.

Special Topic: The General Equation of Degree n

Let K be a field, and let L/K be a field extension.

Definition: $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ are algebraically independent over K if for all $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ such that $g \neq 0$, we have $g(\alpha_1, \ldots, \alpha_n) \neq 0$.

Equivalent Definition: $\alpha_1, \ldots, \alpha_n$ are algebraically independent over K if and only if α_i is transcendental over $K(\alpha_1, \ldots, \alpha_{i-1})$ for all $1 \leq i \leq n$.

Equivalent Definition: $\alpha_1, \ldots, \alpha_n$ are algebraically independent over K if and only if there is a K-isomorphism $\varphi : K(x_1, \ldots, x_n) \to K(\alpha_1, \ldots, \alpha_n)$ with $\varphi(x_i) = \alpha_i$ for $1 \leq i \leq n$.

Definition: For a field K and variables $t_1, t_2, \ldots, t_n$, we denote $K(\bar{t}) := K(t_1, \ldots, t_n)$ (mostly for convenience). The general equation of degree n over K is

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^{n-1} t_{n-1} x + (-1)^n t_n = 0.$$

(If we can solve this general equation by radicals for a given degree n, then we can solve any specific equation with the same degree.)

Example: (Quadratic Formula) Let $\mathrm{char}(K) \neq 2$, and $n = 2$, with $f(x) = x^2 - t_1 x + t_2 = 0$. Then

$$x = \frac{t_1 \pm \sqrt{t_1^2 - 4t_2}}{2}.$$

Proposition V.9.8: Let $n \geq 5$. Then, the general equation of degree n over K cannot be solved by radicals.

Proof: Let $r_1, r_2, \ldots, r_n \in K(\bar{t})^{alg}$ be the roots of $f(x)$. Then,

$$f(x) = \prod_{i=1}^{n} (x - r_i) = x^n - s_1(\bar{r}) x^{n-1} + s_2(\bar{r}) x^{n-2} - \cdots + (-1)^{n-1} s_{n-1}(\bar{r}) x + (-1)^n s_n(\bar{r}).$$

We use $s_j(\bar{r})$ to be the j^{th} elementary symmetric polynomial, evaluated at $(r_1, r_2, \ldots, r_n)$. So,

$$s_j(\bar{r}) = \sum_{i_1 < \cdots < i_j} r_{i_1} r_{i_2} \cdots r_{i_j}.$$

We have that $s_j(\bar{r}) = t_j$, for $1 \leq j \leq n$. Now we will come at the problem from a slightly different direction. We will start with having the r's algebraically independent (we'll call them u's), and see what this then implies about our t's (we'll call them w's).

Let $u_1, \ldots, u_n$ be variables and set $K(\bar{u}) := K(u_1, \ldots, u_n)$. For $1 \leq j \leq n$, set $w_j := s_j(\bar{u})$. Let

$$h(x) = \prod_{i=1}^{n} (x - u_i) = x^n - w_1 x^{n-1} + \cdots + (-1)^{n-1} w_{n-1} x + (-1)^n w_n.$$

In this reformulation, we know that the variables u_i are algebraically independent, but we don't know whether the coefficients w_i are algebraically independent. This is like the opposite of the first part of this proof.

$K(\bar{u})$ is the splitting field of $h(x)$ over $K(\bar{w})$. (Also, $K(\bar{r})$ is the splitting field of $f(x)$ over $K(\bar{t})$.) We know that $\mathrm{Gal}(K(\bar{u})/K(\bar{w})) \cong S_n$. Our goal is now to show an isomorphism between the extensions $K(\bar{t})$ and $K(\bar{w})$.

Define

$$\varphi : K[t_1, \ldots, t_n] \to K[w_1, \ldots, w_n] \text{ defined by } \varphi(g) := g(w_1, \ldots, w_n).$$

By definition φ is surjective ring homomorphism. If $g \in \operatorname{Ker} \varphi$, then

$$0 = \varphi(g) = g(w_1, \ldots, w_n) = g(s_1(\overline{u}), \ldots, s_n(\overline{u})).$$

Now, we evaluate at $u_i = r_i$ for $1 \leq i \leq n$, hence

$$0 = g(s_1(\overline{r}), \ldots, s_n(\overline{r})) = g(t_1, \ldots, t_n).$$

So, $g = 0$. Hence φ is injective. So, φ is an isomorphism.

Let $\widetilde{\varphi} : K(\overline{t}) \to K(\overline{w})$ be the isomorphism induced by φ. Since $f^{\widetilde{\varphi}}(x) = h(x)$ ($\bigstar$), we have that $K(\overline{r})$ is the splitting field of f over $K(\overline{t})$, and $K(\overline{u})$ is the splitting field of h over $K(\overline{w})$, there is an isomorphism $\hat{\varphi} : K(\overline{r}) \to K(\overline{u})$ such that$\hat{\varphi}\big|_{K(\overline{t})} = \widetilde{\varphi}$.

[($\bigstar$) The notation $f^{\widetilde{\varphi}}$ denotes the polynomial you get by applying $\widetilde{\varphi}$ to each coefficient in f.]

Hence

$$\operatorname{Gal}(K(\overline{r})/K(\overline{t})) \cong \operatorname{Gal}(K(\overline{u})/K(\overline{w})) \cong S_n.$$

Since for $n \geq 5$, S_n isn't solvable, so $f(x) = 0$ can't be solved for radicals. $\square$

Application: (Solving a cubic) We first need to assume that $\operatorname{char}(K) \neq 2, 3$.

We show how to solve $f(x) = x^3 + px + q = 0$. We leave out the x^2 term because if there's an Lx^2 term, you can substitute $(x - L)/3$ for x to get rid of it, so we can use this simplification. Now,

$$\begin{aligned} P &= \left(-\frac{q}{2} + \left(\frac{p^3}{27} + \frac{q^2}{4} \right)^{1/2} \right)^{1/3}, \\ Q &= \left(-\frac{q}{2} - \left(\frac{p^3}{27} + \frac{q^2}{4} \right)^{1/2} \right)^{1/3}, \\ PQ &= -\frac{p}{3}. \end{aligned}$$

The choices for P and Q may be somewhat ambiguous because by raising to a fractional power, we must be picking a particular determination of the square or cube roots. But, the third line forces a choice that removes the ambiguities.

Let ω be a primitive cube root of 1. Then, the roots of $f(x)$ are:

$$P + Q, \quad \omega P + \omega^2 Q, \quad \omega^2 P + \omega Q.$$

Example: Let $f(x) = x^3 - 7x + 6 \in \mathbb{Q}[x]$. So, $p = -7$ and $q = 6$. Then,

$$\begin{aligned} P &= \left(-3 + \frac{10}{3\sqrt{3}} i \right)^{1/3} \\ Q &= \left(-3 - \frac{10}{3\sqrt{3}} i \right)^{1/3} \end{aligned}$$

Then, our roots are

$$\begin{aligned} P + Q &= 2 \\ \omega P + \omega^2 Q &= 1 \\ \omega^2 P + \omega Q &= -3. \end{aligned}$$

1.2 Chapter I - Groups

1.2.1 Section I.7 - Categories: Products, Coproducts, and Free Objects

Definition: A category is a class $\mathscr{C}$ of objects such that

(i) For each pair (A, B) of objects, we have a set $\mathrm{Hom}(A, B)$ of morphisms. An element $f \in \mathrm{Hom}(A, B)$ is denoted $f : A \to B$.

(ii) For each triple (A, B, C) of objects, we have a map $\mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$ such that $(g, f) \mapsto g \circ f$, and satisfying the following axioms:

(I) Associativity: If $f : A \to B$, $g : B \to C$, $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.

(II) Identity: For each object $B \in \mathscr{C}$, there exists a morphism $1_B : B \to B$ such that for any $f : A \to B$ and $G : B \to C$, we have that $1_B \circ f = f$ and $g \circ 1_B = g$.

Examples:

(1) $\mathscr{C}$ = the category of sets, morphisms are functions.

(2) $\mathscr{C}$ = the category of groups, morphisms are group homomorphisms.

(3) $\mathscr{C}$ = the category of topological spaces, morphisms are continuous maps.

(4) Let G be a group. Let $\mathscr{C}$ = the category with one object G. The morphisms in this category are the homomorphisms from G to G.

(5) $\mathscr{C}$ = the category of partially ordered sets, morphisms are order-preserving maps.

(6) Let S be a partially ordered set. Let $\mathscr{C}$ = the category whose objects are elements of S. If $a, b \in S$, then there is a unique morphism $f_{a,b} : a \to b$ if and only if $a \leq b$, i.e.,

$$\mathrm{Hom}(a, b) = \begin{cases} f_{a,b}, & \text{if } a \leq b \\ \emptyset, & \text{otherwise} \end{cases}$$

(7) Let $\mathscr{C}$ be a category. Let $\mathscr{D}$ be a new category whose objects are the morphisms in $\mathscr{C}$. A typical object of $\mathscr{D}$ is a morphism $f : A \to B$, where A, B are objects of $\mathscr{C}$ and $f \in \mathrm{Hom}(A, B)$. The morphisms of $\mathscr{D}$ are defined to be the commutative diagrams

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{g} & D \end{array}$$

Now, $\mathrm{Hom}_{\mathscr{D}}(f, g) = \{(\alpha, \beta) \mid \alpha \in \mathrm{Hom}_{\mathscr{C}}(A, C),\ \beta \in \mathrm{Hom}_{\mathscr{C}}(B, D)\}$. For composition of

$$\mathrm{Hom}(g, h) \times \mathrm{Hom}(f, g) \to \mathrm{Hom}(f, h)$$

consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{g} & D \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\delta} \\ E & \xrightarrow{h} & F \end{array}$$

Then, $(\gamma \circ \alpha,\ \ \delta \circ \beta) \in \mathrm{Hom}(f, h)$ is the composition of (γ, δ) with (α, β).

Some common (often conflicting) notations are:

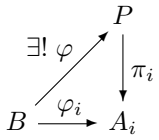
(1) $\mathscr{A}(G)$ = the category of abelian groups.

(2) R-mod = the category of left R-modules (with R a ring).

(3) R-mod = the category of finitely generated left R-modules (with R a ring).

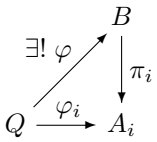
(4) Mod-R = the category of right R-modules (with R a ring).

Definition: Let $\mathscr{C}$ be a category, and let $\{A_i\}_{i\in I}$ be a family of objects of $\mathscr{C}$. A product for this family is an object P of $\mathscr{C}$ together with the morphisms $P \xrightarrow{\pi_i} A_i$, for $i \in I$, such that or any object B and family of morphisms $\varphi : B \to A_i$, with $i \in I$, there is a unique morphism $B \to P$ such that:

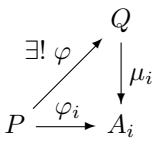


Lemma I.7.3: If P (as in the above definition) exists, then P is unique (up to isomorphism).

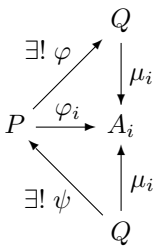
Proof: Let $\{P, \pi_i\}$ and $\{Q, \mu_i\}$ both be products for $\{A_i\}_{i\in I}$. Then applying the definition of P as the product with $B = Q$, we see that there exists a unique homomorphism $\varphi : Q \to B$ such that the diagrams for all i commute:



Applying the definition of Q as the product, with $B = P$, there exists a unique homomorphism $\psi : P \to Q$ such that the diagrams for all i commute:

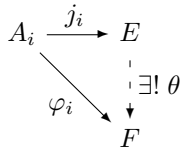


Combining these two diagrams:



The map from Q to Q must be the trivial morphism 1_Q, and so $\psi \circ \varphi = 1_Q$. Similarly $\varphi \circ \psi = 1_Q$. Hence, P and Q are equivalent. □

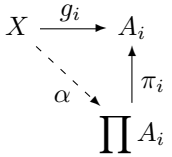
Definition: Let A_i, $i \in I$ be a family of objects in $\mathscr{C}$. A coproduct is an object E together with maps $j_i : A_i \to E$, for $i \in I$ such that if F is an object of $\mathscr{C}$ with maps $A_i \xrightarrow{\varphi_i} F$, there exists unique maps $\theta : E \to F$ such that the following diagram commutes for all i:



Remark: For coproducts, we use the notation $\coprod_{i \in I} A_i$.

Example:

Products: In sets $\prod_{i \in I} A_i$ is the unrestricted direct product $= \{f : I \to \cup A_i \mid f(i) \in A_i\}$, with $\pi_i : (\prod A_i) \to A$, defined by $\pi_i(f) = f(i)$. Suppose we have a set X with maps

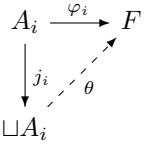


$\alpha : X \to \prod A_i$, with $\alpha(x) = h : j \mapsto g_i(x)$, and $\pi_i(\alpha(x)) = \pi_i(h) = h(j) = g_i(x)$.

Coproduct in Sets: Consider A_i, with $i \in I$. Then

$$\coprod_{i \in I} A_i = \text{ the disjoint union } \bigsqcup_{k \in I} A_k.$$

Let F be a set with maps:



Now we define that θ. Let $x \in \sqcup A_i$, then there exists a unique i with $x \in A_i$. Define $\theta(x) := \varphi_i(x)$. To check this, see that $\theta(j_i(x)) = \varphi_i(x)$.

Abelian Groups:

Product = unrestricted direct product (proof same as for sets)
Coproduct = direct sum = restricted direct product (i.e., only a finite number of nonzero terms in each element)

Groups:

Product = unrestricted direct product
Coproduct = free product (see below)

Remark: It has so far seemed like the product is much bigger than the coproduct. This may trace back to the non-symmetry between the domain and the codomain of a function.

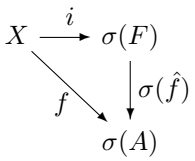
Definition: A concrete category is a category $\mathscr{C}$, together with a σ that assigns to each object of $\mathscr{C}$ a set $\sigma(A)$ in such a way that

(i) Every morphism $A \to B$ of $\mathscr{C}$ is a function of the sets $\sigma(A) \to \sigma(B)$. (Different morphisms must give you different functions. In a category, we can have a bunch of morphisms between the same two sets A and B and thats okay. But, if we treat them as functions from $\sigma(A)$ to $\sigma(B)$, then this cannot happen. So a concrete category must not have multiple morphisms $A \to B$.)

(ii) The identity morphism of A is the identity morphism of $\sigma(A)$.

(iii) Composition of morphisms in $\mathscr{C}$ agrees with composition of functions on the sets $\sigma(A)$, for any object A of $\mathscr{C}$.

Definition: Let F be an object in a concrete category $(\mathscr{C}, \sigma)$. Let $i : X \to \sigma(F)$ be a map of sets. We say that F is free on X if for any object A in $\mathscr{C}$ and any map of sets $f : X \to \sigma(A)$, there exists a unique morphism $\hat{f} : F \to A$ in $\mathscr{C}$ such that:



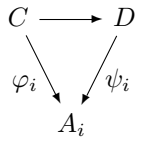
commutes.

Definition: An object I in a category $\mathscr{C}$ is an initial object if for each object A of $\mathscr{C}$, there exists a unique morphism $I \to A$. An object T is a terminal object if for every object C in $\mathscr{C}$, there exists a unique morphism $C \to T$.

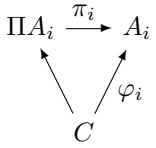
1.2.2 Section I.8 - Direct Products and Direct Sums

We can formulate products, coproducts, free objects, using initial and terminal objects by working in suitable categories.

Remark: Let $\mathscr{C}$ be a category and I a set and $\{A_i\}_{i\in I}$ a family of objects. We consider a new category $\mathscr{D}$, where the objects of $\mathscr{D}$ are families of morphisms $\{C \xrightarrow{\varphi_i} A_i\}_{i\in I}$, where C is an object in $\mathscr{C}$. Morphisms on $\mathscr{D}$ are as follows: If $\{C, \varphi_i\}$ and $\{D, \psi_i\}$ are objects of $\mathscr{D}$, a morphism is a $\mathscr{C}$-morphism $C \to D$ such that all diagrams of the following form commute:



So, a product in the category $\mathscr{C}$ is the same thing as a terminal object in $\mathscr{D}$:

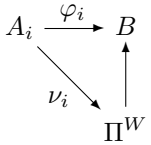


Definition: We construct the weak product (sometimes called direct sum): Define

$$\prod_{i\in I}{}^{W} A_i = \{f : I \to \sqcup A_i\},$$

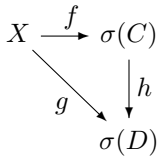
with $f(i) = 0_{A_i}$ for all but finitely many i. This is a coproduct in the category of abelian groups.

Proof: Exercise. Consider diagrams of the form:



1.2.3 Section I.9 - Free Groups, Free Products, and Generators & Relations

Definition: Now we construct free objects similar to before. Let $(\mathscr{C}, \sigma)$ be a concrete category. Let X be a set. We consider a new category $\mathscr{D}$ whose objects are set maps $f : X \to \sigma(C)$, for an object C of $\mathscr{C}$. Morphism of this category are commutative triangles



where $h = \sigma(\varphi)$ for $\varphi \in \hom(C, D)$.

Then, an object F of $\mathscr{C}$ is free on X if and only if F is an initial object in the category $\mathscr{D}$.

Remark: The coproduct in the category of groups is called the free product.

Definition: Let G_i, for $i \in I$ be a family of groups. Let $X := \bigsqcup(G_i)$, and let $\{1\}$ be an extra 1-element set. A word is a sequence $(a_1, a_2, \ldots)$, with $a_i \in X \cup \{1\}$ such that there exists n so that $a_i = 1$ for all $i \geq n$.

Definition: A reduced word is a word that satisfies the following conditions:

(i) No $a_i \in X$ is the identity element in its group G_j.

(ii) For all $i > 1$, a_i and a_{i+1} are not in the same group.

(iii) If $a_k = 1$, then $a_i = 1$ for all $i \geq k$.

Every reduced word can be written uniquely as

$$a_1 \cdots a_n = (a_1, \ldots, a_n, 1, 1, \ldots).$$

Let $\prod_{i \in I}{}^* G_i$ = the set of reduced words. We turn this set into a group by defining product to be concatenation followed by reduction. You have to prove associativity and the other rules by considering all possible cases of cancellation, similar to the case of free groups. The identity element of this group is $1 = (1, 1, \ldots)$.

Proposition: $\prod_{i \in I}{}^* G_i$ is a coproduct with respect to the family $\{G_i\}$ in the set of groups.

Notation: If $I = \{1, \cdots, n\}$, then we write $G_1 * G_2 * G_3 * \cdots * G_n$ for the free product.

1.3 Chapter IV - Modules

1.3.1 Section IV.1 - Modules, Homomorphisms, and Exact Sequences

Definition: Let R be a ring. A (left) R-module is an (additive) abelian group A together with a map $R \times A \to A$ with $(r, a) \mapsto a$, such that for all $r, s \in R$ and $a, b \in A$:

(i) r(a+b) = ra + rb,

(ii) (r+s)a = ra + sa,

(iii) (rs)a = r(sa).

If R has a 1 and if $1a = a$ for all $a \in A$, then we say that A is a unitary or unital R-module.

Definition: Let A be an abelian group. We define the endomorphism ring as

$$\mathrm{End}(A) = \text{ the abelian group homomorphisms from } A \text{ to } A.$$

On this ring $(\varphi + \psi)(a) = \varphi(a) + \psi(a)$ and $(\varphi\psi)(a) = \varphi(\psi(a))$, and these operations do in fact make $\mathrm{End}(A)$ into a ring with 1.

Exercise: With each R-module A, there is naturally associated a ring homomorphism $R \to \mathrm{End}(A)$, and conversely, given any ring homomorphism $R \to \mathrm{End}(A)$, we have a naturally defined R-module structure on A. Also, A is a unital R-module if and only if the homomorphism $R \to \mathrm{End}(A)$ is a homomorphism of rings with units.

Definition: A (left) unital module over a division ring is called a vector space.

Examples and Construction of Modules:

1 Every abelian group is a $\mathbb{Z}$-module. We have $\mathbb{Z} \times A \to A$ with $(r, a) \mapsto ra = \underbrace{a + a + \cdots + a}_{|r| \text{ times}}$ (and the negative of that if r is negative).

2 Every abelian group A is a left $\mathrm{End}(A)$-module. We have $\mathrm{End}(A) \times A \to A$ defined by $(\varphi, a) \mapsto \varphi(a)$.

3 If S is a ring and R is a subring, then S is a left R-module (denoted ${}_RS$) by left multiplication. In particular, S is a left S-module (denoted ${}_SS$) called the left regular module.

Using the left regular module ${}_SS$, we get a homomorphism $S \to \mathrm{End}(S)$. As an exercise, check that this homomorphism is injective (if S is a ring with 1).

4 If I is a left ideal of R, then I is a left R-module. In fact, $\big[\text{left ideals} \equiv R\text{-submodules of } {}_RR\big]$.

5 Let $R \xrightarrow{\varphi} S$ be a ring homomorphism. Then for any S-module M, we obtain an R-module ${}_\varphi M$ by $R \times M \to M$ defined to be $(r, m) \mapsto \varphi(r)m$, with an S-module structure. This called the pullback along φ.

Module Homomorphisms:

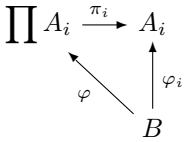
Definition: A module homomorphism for an R-module A to an R-module B is a homomorphism $\varphi : A \to B$ of abelian groups such that $\varphi(ra) = r\varphi(a)$, for all $r \in R$ and $a \in A$.

Remark: Composition of R-module homomorphisms gives a R-module homomorphism.

Remark: R-modules, together with R-module homomorphism, form a category R-Mod.

Products:

Let A_i, for $i \in I$, be a family of (left) R-modules. Then, the cartesian product $\prod A_i$ has a natural R-module structure. Let $f : I \to \bigsqcup A_i$. For $r \in R$, set $(rf)(i) = rf(i)$. Then, since $\prod A_i$ is a product in the category of sets, it follows that it is also a product in R-Mod. This still needs to be checked, but this is the explanation. We need to check that: for $\prod A_i \xrightarrow{\pi_i} A_i$, the π_i are all R-module maps, and that given an object B with a map $B \xrightarrow{\varphi_i} A_i$, for $i \in I$, then since $\prod A_i$ is a product in sets, there exists a unique set map φ from B to $\prod A_i$ such that all the diagrams commute. See the diagram below:



Then we check that φ is an R-module homomorphism.

Coproducts:

In the category of sets, the coproduct is the disjoint union. In the category of groups, the coproduct is the gigantic free product. In the category of abelian groups, the coproduct is the weak direct product (aka, direct sum). Now, for the category of rings, the direct sum $\sum A_i$ (aka, the weak direct product $\prod^W A_i$), *as abelian groups* has a natural R-module structure, and the injections $A_j \xrightarrow{j_i} \sum A_i$ are R-module homomorphism. Moreover, given any R-module homomorphism $A_j \xrightarrow{\varphi_j} B$, the unique homomorphism (of abelian groups) $\sum A_i \xrightarrow{\varphi} B$ in the definition of the coproduct of abelian groups is in fact an R-homomorphism. So, it follows that $\sum A_i$ is a coproduct in the category R-Mod.

Definition: If R is a ring (may not have 1), let A be a (left) R-module. Let $a \in A$. The cyclic submodule of A generated by a is the intersection of all submodules containing a.

Proposition IV.1.5a:

(1) If R has a 1, then the cyclic submodule generated by a is cyclic: $Ra = \{ra \mid r \in R\}$.

(2) If R does not have a 1, then the cyclic submodule generated by a is: $\{ra + na \mid r \in R, n \in \mathbb{Z}\}$.

Definition: We say that A is cyclic if A is generated by a single element. If $X \subseteq A$, then the submodule generated by X is the intersection of all submodules containing X.

Proposition IV.1.5b:

(1) The submodule generated by $X = \{\sum r_i x_i + \sum n_t g_t \mid r_i \in R, x_i \in X, n_t \in \mathbb{Z}, y_t \in X\}$.

(2) If R has a 1, then it simplifies to $\{\sum r_i x_i \mid r_i \in R, x_i \in X\}$.

Theorem: If R is a ring without 1, then we can embed R into a ring S with 1 such that $S \cong R \oplus \mathbb{Z}$ as abelian groups. (If $\operatorname{char} R = n$, we can replace $\mathbb{Z}$ by $\mathbb{Z}/n\mathbb{Z}$.)

> **Proof:** Let $S = R \oplus \mathbb{Z}$. Define addition: $(r_1, n_1) + (r_2, n_2) = (r_1 + r_2, n_1 + n_2)$. Define multiplication: $(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1 r_2 + n_2 r_1, n_1 n_2)$. It's not too hard to check that these two operations together with the identity $(0, 1)$ make S a ring. □

Exact Sequences

Definition: If you have homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$, we say this sequence is exact at B if and only if $\operatorname{Im} f = \operatorname{Ker} g$. A short exact sequence is a sequence of maps $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} 0$ which is exact at A, B, C. I.e., $\operatorname{Ker} f = 0$, $\operatorname{Im} f = \operatorname{Ker} g$, $\operatorname{Im} g = \operatorname{Ker} h = C$. So, $\operatorname{Im} f \cong A$ and $B/\operatorname{Im} f = B/\operatorname{Ker} g \cong \operatorname{Im} g = C$. Exact sequences have analogous definitions in other categories.

Lemma IV.1.17: Suppose we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

of R-module maps such that each row is exact. Then,

(i) α, γ are (injective) monomoprhisms $\Longrightarrow \beta$ is a monomorphism.

(ii) α, γ are (onto) epimorphisms $\Longrightarrow \beta$ is an epimorphism.

(iii) α, γ are isomorphism $\Longrightarrow \beta$ is an isomorphism.

> **Proof:** Let $x \in \operatorname{Ker} \beta$. Then, $\beta(x) = 0$, and so $g'\beta(x) = 0$. Thus $\gamma g(x) = 0$ because the diagram commutes. So $g(x) = 0$ since γ is a monomorphism. Thus $x = f(a)$ for some $a \in A$ since the row is exact. Hence $0 = \beta(x) = \beta f(a) = f'\alpha(a)$, since the diagram commutes. So $a = 0$ since f' and α are monomorphism. Thus, $x = f(a) = 0$. So β is a monomorphism. The proofs for other parts are similar. □

Definition: Two short exact sequences are said to be isomorphic if there is a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

such that f, g, and h are isomorphisms. The same diagram going backward with the inverse maps is also commutative and so has the same isomorphism. Thus this notion of isomorphism is an equivalence relation.

Theorem IV.1.18: Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of (left) R-modules. Then, the following are equivalent:

(i) There exists an R-module map $h : C \to B$ such that $gh = 1_C$.

(ii) There exists an R-module map $k : B \to A$ such that $kf = 1_A$.

(iii) The short exact sequence is isomorphic to $0 \to A \xrightarrow{i_a} A \oplus C \xrightarrow{\pi_i} C \to 0$ (with $i_A(a) := (a, 0)$ and $\pi_C(a, c) := c$ for all $a \in A, c \in C$.

A short exact sequence that satisfies these conditions is called a split short exact sequence.

Proof:
(i) $\Longrightarrow$ (iii):

Let $D = \operatorname{Im} h$. Claim $B \cong \operatorname{Im} f \oplus D$.

Let $b \in B$. Then, $g(b - hg(b)) = g(b) - ghg(b) = g(b) - g(b) = 0$.
So, $b - hg(b) \in \operatorname{Ker} g = \operatorname{Im} f$. Hence, $B = \operatorname{Im} f + D$.

On the other hand, if $b \in \operatorname{Im} f \cap D$, then $b \in \operatorname{Ker} g \cap \operatorname{Im} h$, so $b = h(c)$ for some c. Then, $0 = g(b) = gh(c) = 0$. Thus $c = 0$ and so $b = 0$. Hence, $\operatorname{Im} f \cap D = \{0\}$. Now we have the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \| & & \uparrow & & \| & & \\
 & & = & & f(A) \oplus hC & & = & & \\
 & & \| & & \cong \uparrow & & \| & & \\
0 & \longrightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{\pi} & C & \longrightarrow & 0
\end{array}$$

with $\alpha : A \oplus C \to B$ defined by $\alpha(a, c) := (f(a), h(c))$. We've shown that α is an isomorphism, and from definitions we see that the diagram commutes.

(iii) $\Longrightarrow$ (i):

$$\begin{array}{ccccccccc}
 & & & & & \overset{h}{\leftarrow\!\!\rightarrow} & & & \\
0 & \longrightarrow & A & \longrightarrow & B & & C & \longrightarrow & 0 \\
 & & \beta \uparrow \cong & & \alpha \uparrow \cong & & \gamma \uparrow \cong & & \\
 & & | & & | & \overset{i_C}{\rightarrow\!\!\leftarrow} & | & & \\
0 & \longrightarrow & A & \longrightarrow & A \oplus C & & C & \longrightarrow & 0 \\
 & & & & & \underset{\pi}{\leftarrow\!\!\rightarrow} & & &
\end{array}$$

Define $h := \alpha \circ i_C \circ \gamma^{-1}$. Then

$$\begin{aligned}
gh(c) &= (g\alpha i_C \gamma^{-1})(c) \\
&= (\gamma \pi i_C \gamma^{-1})(c) \\
&= (\gamma(1_C)\gamma^{-1})(c) \\
&= c.
\end{aligned}$$

(ii) $\Longrightarrow$ (iii):

Consider the short exact sequence

$$0 \longrightarrow A \underset{k}{\overset{f}{\rightleftarrows}} B \xrightarrow{g} C \longrightarrow 0$$

with $kf = 1_A$.

Let $D := \operatorname{Ker} K$. Claim $B = \operatorname{Im} f \oplus D$. Let $b \in B$. Then $k(b - fk(b)) = k(b) - kfk(b) = k(b) - k(b) = 0$. Hence $b - fk(b) \in D$, and so $b \in \operatorname{Im} f + D$.

Let $b \in \operatorname{Im} f \cap \operatorname{Ker} k$. Then, $b = f(a)$ for some a. So, $0 = k(a) = kf(a) = a$, hence $a = 0$ and thus $b = 0$. Therefore, $\operatorname{Im} f \cap \operatorname{Ker} k = \{0\}$. Thus, $B = \operatorname{Im} f \oplus \operatorname{Ker} k$.

Now consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow = & & \downarrow \cong & & \downarrow = & & \\
 & & & & f(A) \oplus \operatorname{Ker}(k) & & & & \\
 & & & & k \downarrow & g|_{\operatorname{Ker}(k)} & & & \\
0 & \longrightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{\pi} & C & \longrightarrow & 0
\end{array}$$

1.3.2 Section IV.2 - Free Modules and Vector Spaces

Definition: Let R be a ring, and let A be an R-module. A subset X of A is linearly independent provided that for distinct $x_1, \cdots, x_n \in X$, and (not necessarily distinct) elements $r_1, \cdots, r_n \in R$, we have that

$$[r_1x_1 + \cdots + r_nx_n = 0] \Longrightarrow [\forall i : r_i = 0] .$$

Definition: We say that a subset $Y \subseteq A$ spans A if A is generated by Y.

Definition: A linearly independent set that also spans A is called a basis of A.

Theorem IV.2.1: Let R be a ring with 1. Let F be a unital R-module. Then, the following are equivalent:

(i) F has a nonempty basis.

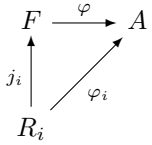
(ii) F is the internal direct sum of a family of cyclic R-modules, each $\cong {}_RR$.

(iii) F is isomorphic to a direct sum of copies of ${}_RR$.

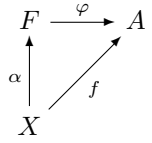
(iv) There exists a nonempty set X and a function $i : X \to F$ satisying the Universal Mapping Property of a free object in the category of (left) R-modules.

Proof:
(iii) $\Longleftarrow$ (iv):

Suppose $F \cong \sum_{i \in X} R_i$ (this is the direct sum, i.e., the coproduct), where $R_i \cong {}_RR$. Let $j_i : R_i \to F$ be the inclusion map. Let $x_i \in R_i$ be a generator of R_i. Let $\alpha : X \to F$ send $i \mapsto j_i(x_i)$. Let A be any R-module, and suppose we are given $a_i, i \in I$, elements of A. Then, for each i, there exists a unique homomorphism $\varphi_i : R_i \to A$ defined by $\varphi_i : x_i \mapsto a_i$. Then, by the universal property of coproducts, there exists a unique homomorphism of R-modules $\varphi : F \to A$ such that



Let $f : X \to A$ be any set map. Set $a_i = f(i)$, for all $i \in X$. Then,



with $\varphi(j(x_i)) = \varphi(\alpha(i)) = f(i)$. Hence F is free on X. $\square$

1.3.3 Section IV.3 - Projective and Injective Modules

Projective and Injective Modules:
Assume R has a 1. We consider (left) unital R-modules.

Definition: An R-module P is projective if every diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle g} & & \\ A & \xrightarrow{f} & B & \longrightarrow & 0 \end{array}$$

with an exact row can be completed to a commutative diagram by a map h (represented by a dotted arrow):

$$\begin{array}{ccccc} & & P & & \\ & \overset{\exists h}{\swarrow} & \downarrow{\scriptstyle g} & & \\ A & \xrightarrow{f} & B & \longrightarrow & 0 \end{array}$$

We make no assertions about the uniqueness of h, just the existence.

Theorem IV.3.4: For a left R-module P, the following are equivalent:

(1) P is projective.

(2) Every short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow P \longrightarrow 0$$

splits.

(3) There exists a free module F and a module K such that $F \cong K \oplus P$.

Proof:
(1) $\Longrightarrow$ (2):

Consider the short exact sequence:

$$0 \longrightarrow A \longrightarrow B \xrightarrow{f} P \longrightarrow 0$$

By the definition of projectivity, there exists a map $h : P \to B$ such that $f \circ h = \mathrm{Id}_P$. Then, we have the diagram:

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \overset{\exists h}{\swarrow} & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & P & \longrightarrow & 0 \end{array} \quad \mathrm{Id}$$

So, the sequence splits. $\square$

(2) $\Longrightarrow$ (3):

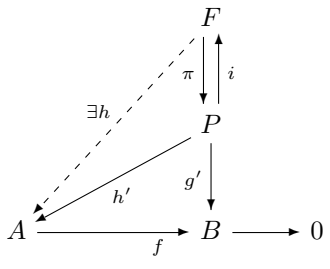
There exists F free and a surjective homomorphism $f : F \to P$. So, we have the short exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$$

where $K = \operatorname{Ker} f$. By hypothesis, this splits, do $F \cong K \oplus P$. $\square$

(3) $\Longrightarrow$ (1):

Let $F \cong K \oplus P$, with $i : P \to F$ and $\pi : F \to P$. Set $h' = h \circ i$. We have the diagram:



We have that

$$f \circ h' = f \circ h \circ i = (g \circ \pi) \circ i = g \circ 1_P = f. \ \square$$

Example: Consider

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Let $R = \mathbb{Z}/6\mathbb{Z}$. Then, $\mathbb{Z}/6\mathbb{Z}$ is a free R -module, so $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ are projective (but not free) R-modules.

Proposition IV.3.5: A direct sum of R-modules $\sum_{i \in I} P_i$ is projective if and only if each P_i is projective.

Proof:
($\Longrightarrow$) :

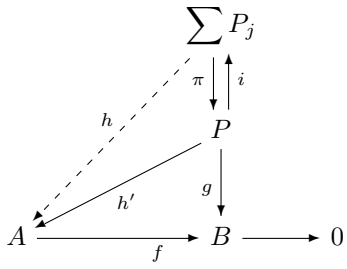
Suppose $\sum_{j \in I} P_j$ is projective. Let

$$i : P_k \to \sum P_j$$

$$\pi : \sum P_j \to P_k$$

be the canonical maps.

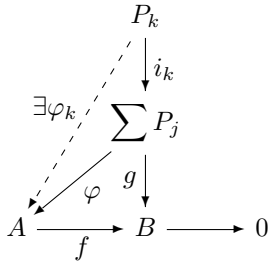
Letting $h' = h \circ i$, we have the following diagram:



Thus P is projective. $\square$

($\Longleftarrow$) :

Now, assume each P_j is projective. By the definition of $\sum P_j$ as a coproduct, there exists $\varphi : \sum P_j \to A$ such that every triangle commutes. So we have the following diagram:

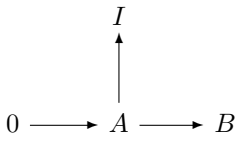


We want to show that $f \circ \varphi = g$.

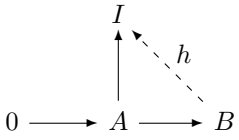
Since the $i_k(P_k)$ generate $\sum P_j$, it suffices to show that $f \circ \varphi \circ i_k = g \circ i_k$. But $\varphi \circ i_k = \varphi_k$ and $f \circ \varphi_k = g \circ i_k$ by commutativity. $\square$

Injective Modules:

Definition: A left R-module is injective if every diagram



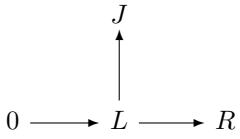
can be completed by a map (given by the dotted arrow) to a commutative diagram.



Proposition IV.3.7:: A direct product $\prod_{j \in I} J_i$ is injective if and only if each J_i is injective.

Proof: Exercise.

Lemma IV.3.8: Let R be a ring with 1. A unitary R-module J is injective if and only if for any left ideal L of R, any R-module map $L \to J$ can be extended to an R-module map from $R \to J$, as in the diagram:

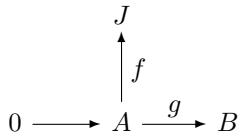


Proof:
($\Longrightarrow$):

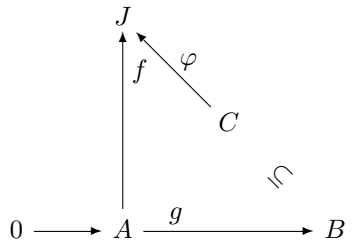
If J is injective, then the diagram above can be completed. $\square$

($\Longleftarrow$):

Consider the diagram

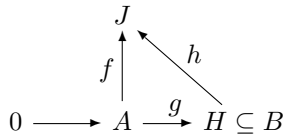


We consider pairs (C, φ) where $g(A) \subseteq C \subseteq B$ and $\varphi \circ g = f$:



Call the set of all such pairs ζ. Then $\zeta \neq \emptyset$ since $(g(A), f \circ g^{-1}) \in \zeta$ (since g is injective). Partially order this set by map extension.

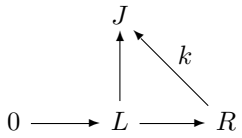
By **Zorn's Lemma**, there exists a maximal element $(H, h) \in \zeta$.



We claim that $H = B$. Suppose not. Let $b \in B \setminus H$. We'll extend the map h to $\langle H, G\rangle$ to contradict the maximality of H.

Let $L = \{r \in R \mid rb \in H\}$. L is a left ideal. Define $L \to J$ by $r \mapsto h(rG)$. Needs to be checked that this an R-module map.

By hypothesis, this extends to an R-module map $k : R \to J$:



Since R has a 1, we can let $c \in k(1_R)$.

Define $\overline{h} : \langle H, G\rangle \to J$ by $\overline{h}(a + rb) = h(a) + rc$. If this is an R-module map, then we have extended h. However, we don't know that it's a well-defined R-module map, so this needs to be checked, by showing: If $a_1 + r_1 b = a_2 + r_2 b$, then $h(a_1) + r_1 c = h(a_2) + r_2 c$.

Suppose $a_1 + r_1 b = a_2 + r_2 b$. Then, $a_1 - a_2 = (r_2 - r_1)b \in H$, hence $r_2 - r_1 \in L$. So,

$$h(a_1) - h(a_2) = h(a_1 - a_2) = h((r_2 - r_1)b) = k(r_2 - r_1) = k(r_2) - k(r_1) = r_2 k(1) - r_1 k(1) = r_2 c - r_1 c.$$

Hence, $h(a_1) + r_1(c) = h(a_2) + r_2(c)$. Thus the map is well-defined.

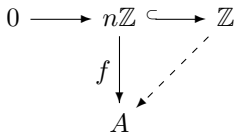
Check that $\overline{h}$ is in fact an R-module map. Then, $\overline{h}$ is an R-module map extending h, which is a contradiction to the maximality. $\square$

Definition: Recall that unital $\mathbb{Z}$-modules are equivalent to abelian groups. We say that an abelian group D is divisible if given any $y \in D$ and $0 \neq n \in \mathbb{Z}$, there exists $x \in D$ such that $nx = y$.

Lemma IV.3.9: An abelian group is an injective $\mathbb{Z}$-module if and only if it is divisible.

Proof:
($\Longrightarrow$):

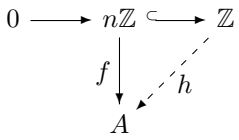
Consider the diagram:



with $f : n\mathbb{Z} \to A$ and $n \mapsto a$. Suppose A is injective. Then, one can extend f to $h : \mathbb{Z} \to A$ and let $y = h(1)$. Then, $ny = nh(1) = h(n) = f(n) = a$, and so A is divisible.

($\Longleftarrow$):

Suppose A is divisible. Then, for any diagram:



with $f(n) = a$ and n, a arbitrary with $n \in \mathbb{Z} \setminus \{0\}$ and $a \in A$, the diagram can be completed. But, all left ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some n, and all maps $f : n\mathbb{Z} \to A$ map n to some $a \in A$. So, by **Lemma IV.3.8**, A is injective. □

Lemma IV.3.10: Every abelian group can be embedded into an injective (divisible) module.

Lemma IV.3.11: If J is a divisible abelian group and R is a ring with identity, then $\mathrm{Hom}_{\mathbb{Z}}(R, J)$ is an injective left R-module.

Proof: Let R be a ring with 1 and let J be a divisible $\mathbb{Z}$-module. Define for $r \in R$ and $f \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$ that $(rf)(x) := f(xr)$ for all $x \in R$.

Now we need to check:

(1) $rf \in \mathrm{Hom}_{Z}(R, J)$:

$$(rf)(x \cdot y) = f((x \cdot y)r) = f(xr + yr) = f(xr) + f(yr) = (rf)(x) + (rf)(y).$$

(2) Module structure: for $f, g \in \mathrm{Hom}_{\mathbb{Z}}(R, J)$ and $r, s \in R$

(-) $r(f + g) = rf + rg$, and $1f = f$.

(-) $(rs)f(x) = f(x(rs)) = f((xr)s) = ((sf)r)(x) = (r(sf))(x)$.

Proposition IV.3.12: Every unitary left R-module can be embedded into an injective R-module.

Proof: Let A be a left unitary R-module. We can embed A into an injective abelian group J as

$$R \xrightarrow{g} A \overset{f}{\hookrightarrow} J$$

Now, consider the map

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}}(R, A) &\xrightarrow{\overline{f}} \mathrm{Hom}_{\mathbb{Z}}(R, J) \\ g &\longmapsto f \circ g \end{aligned}$$

Note that $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ is an R-module map and that there is a canonical isomorphism between A and $\mathrm{Hom}_R(R, A)$ and that $\mathrm{Hom}_R(R, A) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, A)$. It remains to check that $\overline{f}$ is an R-module map. $\square$

1.3.4 Section IV.4 - Hom and Duality

In this section, we consider only unital rings. In the case of a nonunital ring, you can embed that ring into a unital ring for which the modules are the same.

Definition: If A and B are left R-modules, then

$$\mathrm{Hom}_R(A,B) := \{R\text{-module maps from } A \text{ to } B\}.$$

$\mathrm{Hom}_R(A,B)$ has the structure of an abelian group: $(\varphi+\psi)(a) = \varphi(a)+\psi(a)$.

Induced Maps: Consider the diagram:

$$A \xrightarrow{g} B \xrightarrow{f} C$$

Then, we can find a map:

$$\begin{array}{ccc} \mathrm{Hom}_R(A,B) & \xrightarrow{\widetilde{f}} & \mathrm{Hom}_R(A,C) \\ g & \longmapsto & f\circ g \end{array}$$

and a map:

$$\begin{array}{ccc} \mathrm{Hom}_R(B,C) & \xrightarrow{\widetilde{g}} & \mathrm{Hom}_R(A,C) \\ h & \longmapsto & h\circ g \end{array}.$$

These two induced maps are abelian group homomorphisms.

Theorem IV.4.2: (left exactness of Hom, covariant version) Let R be a ring. Then

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$$

is an exact sequence of R-modules if and only if for every R-module D:

$$0 \longrightarrow \mathrm{Hom}_R(D,A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D,B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_r(D,C)$$

is exact.

Proof:
($\Longrightarrow$):

First we show that $\overline{\varphi}$ is injective. Let

$$D \xrightarrow{f} A \xrightarrow{\varphi} B$$

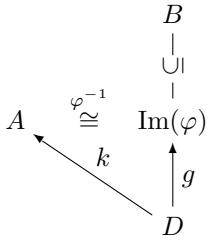
and define

$$\begin{array}{ccc} \mathrm{Hom}_R(D,A) & \xrightarrow{\overline{\varphi}} & \mathrm{Hom}_R(D,B) \\ f & \longmapsto & \varphi\circ f \end{array}$$

Suppose $\overline{\varphi}(f) = 0$. Then, $\varphi\circ f = 0$. Since φ is injective, we have $f = 0$. Hence $\overline{\varphi}$ is injective.

Now we show $\mathrm{Im}(\overline{\varphi}) \subseteq \mathrm{Ker}(\overline{\psi})$. Suppose $g \in \mathrm{Im}(\overline{\varphi})$. Then $g = \varphi\circ f$ for some $f \in \mathrm{Hom}_R(D,A)$. Then, $\overline{\psi}(g) = \psi\circ g = \psi\circ\varphi\circ f = 0$ (since $\psi\circ\varphi = 0$).

Now we show that $\mathrm{Ker}(\overline{\psi}) \subseteq \mathrm{Im}(\overline{\varphi})$. Let $g \in \mathrm{Ker}(\overline{\psi})$. Then $\psi \circ g = 0$. So $\mathrm{Im}(g) \subseteq \mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$. But, $\mathrm{Im}(\varphi) \cong A$ (by injectivity), so let $k \in \mathrm{Hom}_R(D, A)$ be defined by $\varphi^{-1} \circ g$ (see diagram)



Then, $\overline{\varphi}(k) = \varphi \circ k$. Now, $\overline{\varphi}(k)(d) = \varphi(\varphi^{-1}(g(d))) = g(d)$, for all $d \in D$. So, $\overline{\varphi}(k) = g$. $\square$

($\Longleftarrow$):

Conversely, assume

$$0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C)$$

is exact for all R-modules D.

First we show φ is injective. Let $D = {}_RR$. Let $f \in \mathrm{Hom}_R(R, A)$ be the unique R-module map sending 1 to a. Let $a \in \mathrm{Ker}(\varphi)$. Then, $\overline{\varphi}(f)(1) = \varphi(f(1)) = \varphi(a) = 0$. Hence, $f \in \mathrm{Ker}(\overline{\varphi})$ and so $f = 0$. Hence $a = 0$.

Now we show $\mathrm{Im}(\varphi) \subseteq \mathrm{Ker}(\psi)$. Use $D = {}_RR$. Let $b \in \mathrm{Im}(\varphi)$. Let $f \in \mathrm{Hom}_R(R, B)$ be the unique R-module map sending 1 to b. Then, $b = \varphi(a)$ for some $a \in A$. So, $f(1) = \varphi(a)$. Let $g \in \mathrm{Hom}_R(R, A)$ be the unique R-module map sending 1 to a. Then, $f(1) = \varphi(a) = \varphi(g(1))$. Since maps in $\mathrm{Hom}_R(R, B)$ are determined by the image of 1, we see that $f = \varphi \circ g = \overline{\varphi}(g)$. By exactness of the induced sequence at $\mathrm{Hom}_R(D, B)$, we have that $f \in \mathrm{Ker}\,\overline{\psi}$. Therefore $\psi \circ f = 0$. Hence, $\psi(f(1)) = 0$, and so $b = f(1) \in \mathrm{Ker}(\psi)$.

Now we show $\mathrm{Ker}(\psi) \subseteq \mathrm{Im}(\varphi)$. Again let $D = {}_RR$. Let $b \in \mathrm{Ker}(\psi)$. Let $f \in \mathrm{Hom}(R, B)$ be the unique R-module map sending 1 to b. Then, $0 = \psi(b) = \psi(f(1))$. So $\psi \circ f = 0$. So, $f \in \mathrm{Ker}(\overline{\psi}) \subseteq \mathrm{Im}(\overline{\varphi})$. So, there exists $g \in \mathrm{Hom}_R(R, A)$ such that $\overline{\varphi}(g) = f$, i.e., $f = \varphi \circ g$. $\square$

Proposition IV.4.3: (left exactness of Hom, contravariant version) Let R be a ring. Then, the sequence

$$A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

of R-modules is exact if and only if for any R-module D

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A, D)$$

is exact.

Proof: Exercise.

Proposition IV.4.4: The following are equivalent:

(1) $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is a split exact sequence of R-modules.

(2) $0 \longrightarrow \mathrm{Hom}_R(D,A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D,B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D,C) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D.

(3) $0 \longrightarrow \mathrm{Hom}_R(C,D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B,D) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A,D) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D.

Proof:
(1) $\Longrightarrow$ (3) :

It suffices to check that $\overline{\varphi}$ is surjective, by left exactness of Hom. Let $f \in \mathrm{Hom}_R(A,D)$. We want to show that there exists $g \in \mathrm{Hom}_R(B,D)$ such that $\overline{\varphi}(g) = f$, i.e., $g \circ \varphi = f$. By hypothesis, there exists $k : B \to A$ such that $K \circ \varphi = \mathrm{Id}_A$. Let $g = f \circ k : B \to D$. Then $g \circ \varphi = f \circ k \circ \varphi = f \circ \mathrm{Id}_A = f$. This shows that the sequence in (3) is exact. It remains to show that it splits. This is left as an exercise to whoever reads these notes.

Other directions are similar.

Theorem IV.4.5: The following conditions on an R-module P are equivalent:

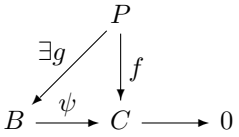
(1) P is projective.

(2) If $\psi : B \to C$ is any surjective R-module map, then $\overline{\psi} : \mathrm{Hom}_R(P,B) \to \mathrm{Hom}_R(P,C)$ is surjective.

(3) If $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is a short exact sequence of R-modules, then
$0 \longrightarrow \mathrm{Hom}_R(P,A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(P,B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P,C) \longrightarrow 0$ is exact.

Proof:
(1) $\Longrightarrow$ (2):

We have the diagram:



with $f \in \mathrm{Hom}_R(P,C)$, $g \in \mathrm{Hom}_R(P,B)$ and $f = \psi \circ g$.

(1) $\Longrightarrow$ (3):

Suppose we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

Then,

$$0 \longrightarrow \mathrm{Hom}_R(P,A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(P,B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P,C) \longrightarrow 0$$

is exact by left exactness, and $\overline{\psi}$ is surjective by projectivity.

(3) $\Longrightarrow$ (1):

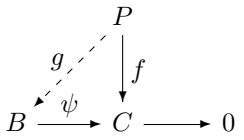
Suppose

$$0 \longrightarrow \mathrm{Hom}_R(P, A) \longrightarrow \mathrm{Hom}_R(P, B) \longrightarrow \mathrm{Hom}_R(P, C) \longrightarrow 0$$

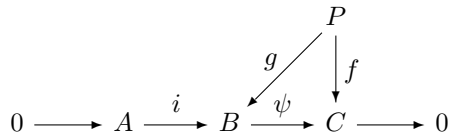
is exact for any short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

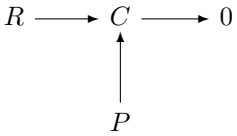
Let



be given. The function g on the dashed line is defined below. Let $A = \mathrm{Ker}\,\psi$. Then, we have a short exact sequence



By surjectivity of $\overline{\psi}$, there exists $g \in \mathrm{Hom}_R(P, B)$ such that $\psi \circ g = f$. Then since this holds for all



we have that P is projective.

Other direction similar to the above three.

Theorem IV.4.6: The following conditions are equivalent on an R-module J:

(1) J is injective.

(2) If $\sigma : A \to B$ is any injective map of R-modules, then $\overline{\sigma} : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$ is surjective.

(3) If

$$0 \longrightarrow A \xrightarrow{\sigma} B \xrightarrow{\zeta} C \longrightarrow 0$$

is a short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(C, J) \longrightarrow \mathrm{Hom}_R(B, J) \longrightarrow \mathrm{Hom}_R(A, J) \longrightarrow 0$$

is exact.

Theorem IV.4.7: Let $A, B, \{A_i\}_{i\in I}, \{B_j\}_{j\in J}$ be R-modules. Then, we have isomorphisms of abelian groups:

(i)
$$\mathrm{Hom}_R\left(\sum_{i\in I} A_i,\ \ B\right) = \prod_{i\in I} \mathrm{Hom}_R(A_i, B)$$

(ii)
$$\mathrm{Hom}_R\left(A,\ \prod_{j\in J} B_j\right) = \prod_{j\in J} \mathrm{Hom}_R(A, B_j)$$

Proof of (i): Consider the diagram:

$$A_i \xhookrightarrow{i_i} \sum_{i\in I} A_i \xrightarrow{f} B$$

So, we have a map

$$\pi_i : \mathrm{Hom}_R\left(\sum_{i\in I} A_i, B\right) \to \mathrm{Hom}_R(A_i, B)$$

defined by $f \mapsto f \circ i_i$. Now suppose we have an abelian group C with maps $f_i : C \to \mathrm{Hom}_R(A_i, B)$, for $i \in I$. Define $f : C \to \mathrm{Hom}_R\left(\sum_{i\in I} A_i, B\right)$ as follows: for $c \in C$, let $f(c)$ be the map

$$[f(c)]\left(\sum_{i\in I} a_i\right) := \sum [f_i(c)](a_i).$$

We need to check that for all $c \in C$, the map $f(c)$ is a homomorphism. We also need to check that f is a homomorphism. Lastly, we need to check the $\pi_i \circ f = f_i$. These are easy to check. □

Bimodules

Definition: Let R, S be rings. An (R, S)-bimodule is an abelian group M such that

(1) M is a left R-module,

(2) M is a right S-module,

(3) For all $r \in R$, $s \in S$, $m \in M$, we have that $r(ms) = (rm)s$.

To indicate that M is an (R, S)-bimodule, we write ${}_RM_S$.

Examples:

(1) A ring acting on itself (i.e. ${}_RR_R$) is an (R, R)-bimodule. The two-sided ideals of R are the (R, R)-submodules.

(2) If R is commutative, every left module can be made into a bimodule by defining

$$m \cdot r := rm.$$

(3) Every left R-module is an $(R, \mathbb{Z})$-module.

Theorem IV.4.8: Consider ${}_RA$, ${}_RA'$, ${}_RB_S$, ${}_RC_S$, and ${}_RS$.

(1) $\mathrm{Hom}_R(A,B)$ is a right S-module, with action $(fs)(a) = f(a)s$.

(2) If $\varphi : A \to A'$ is an R-module map, then $\overline{\varphi} : \mathrm{Hom}_R(A',B) \to \mathrm{Hom}_R(A,B)$ defined by $\overline{\varphi} : f \mapsto f \circ \varphi$ is a right S-module map.

(3) $\mathrm{Hom}_R(C,A)$ is a left S-module map, with action $(sf)(c) = cf(s) = f(cs)$.

(4) If $D \xrightarrow{\psi} D'$ is an R-module map, then $\mathrm{Hom}_R(C,D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(C,D')$ defined by $f \mapsto \psi \circ f$ is a left S-module homomorphism.

Checking (3):

$(s'(sf))(c) = (sf)(cs') = f((cs')s) = f(c(s's)) = f(c(ss')) = (ss')f(c) = ((ss')f)(c)$. Hence $s'(sf) = (s's)f$.

Checking (4):

$\overline{\psi}(sf)(c) = \psi \circ (sf)(c) = \psi(f(cs)) = (\overline{\psi}f)(cs) = (s(\overline{\psi}f))(c)$. Hence $\overline{\psi}(sf) = s\overline{\psi}(f)$.

Theorem IV.4.9: Let A be a left unitary R-module, and R a ring with 1. Then,

$$\mathrm{Hom}_R(R,A) \cong A$$

as R-modules, by the isomorphism $[f_a : 1_R \mapsto a] \leftarrow\!\shortmid a.$, and $f \mapsto f(1)$.

Proof: Exercise.

Duality:

Definition: Let A be a left R-module, so we have ${}_RA$ and ${}_RR_R$. Then, $A^* := \mathrm{Hom}_R(A,R)$ is a right R-module called the dual of A.

Theorem IV.4.10: Let A, B, C be left R-modules.

(1) If $\varphi : A \to C$ is an R-module map, then $\overline{\varphi} : \mathrm{Hom}_R(C,R) \to \mathrm{Hom}_R(A,R)$ is an right R-module map.

(2) $(A \oplus C)^* \cong A^* \oplus C^*$.

(3) If R is a division ring and $0 \longrightarrow A \xrightarrow{\sigma} B \xrightarrow{\xi} C \longrightarrow 0$ is a short exact sequence of left R-modules, then $0 \longrightarrow A^* \xrightarrow{\overline{\xi}} B^* \xrightarrow{\overline{\sigma}} A^* \longrightarrow 0$ is a short exact sequence of right R-modules.

Theorem IV.4.11: Let F be a free left module with basis X over a ring R with 1. For $x \in X$, set $f_x : F \to R$ be the homomorphism such that for $y \in X$:

$$f_x(y) = \delta_{xy} = \begin{cases} 1, & \text{if } y = x \\ 0, & \text{if } y \neq x \end{cases}$$

Then,

(1) $\{f_x \mid x \in X\}$ is a linearly independent set in F^*.

(2) If X is finite, then F^* is a free right module with basis $\{f_x \mid x \in X\}$.

Proof: Exercise.

Theorem IV.4.12: There is a left R-module homomorphism:

$$\theta : A \to A^* *$$

defined by $\theta(a)(f) = f(a)$, for all $a \ni A$ and $f \in A^*$.

If R has a 1 and A is free then θ is injective.

If R has a 1 and A is free with a finite basis, then θ is an isomorphism.

1.3.5 Section IV.5 - Tensor Products

If A_R and ${}_RB$, we will define an abelian group $A \otimes_R B$.

Definition: Let C be an abelian group. A map $f : A \times B \to C$ is called an R-middle-linear map if

(1) f is $\mathbb{Z}$-linear:

$$f(a + a', b) = f(a, b) + f(a', b),$$

$$f(a, b + b') = f(a, b) + f(a, b').$$

(2) $f(ar, b) = f(a, rb)$, for all $a \in A$, $b \in B$, $r \in R$.

For fixed A_R and ${}_RB$, we consider the category $\mathscr{M}(A, B)$ whose objects are the middle-linear maps $A \times B \to C$, where C is an abelian group. The morphisms in this category are commutative diagrams:

$$\begin{array}{ccc} A \times B & \xrightarrow{f} & C \\ \downarrow{\scriptstyle g} & \nearrow_{h} & \\ D & & \end{array}$$

where h is the morphism, so that

$$(A \times B \xrightarrow{f} C) \xrightarrow{h} (A \times B \xrightarrow{g} D).$$

Definition: A universal object of $\mathscr{M}(A, B)$ is called a tensor product $A \otimes_R B$. By the definition of a universal object, if this tensor product exists it must be unique.

Remark: Note that this is a (slight) abuse of notation, since the objects are realy maps $A \times B \to A \otimes_R B$, for which there is a canonical mapping $(a, b) \mapsto a \otimes_R b$.

Universal Property of $A \otimes_R B$:

> There exists a middle-linear map $A \times B \to A \otimes_R B$ such that for any abelian group C and any middle-linear map f from $A \times B$ to C, there exists a unique $\widetilde{f} : A \otimes_R B \to C$.
>
> $$\begin{array}{ccc} A \times B & \xrightarrow{f} & C \\ {\scriptstyle j}\downarrow & \nearrow_{\widetilde{f}} & \\ A \otimes_R B & & \end{array}$$
>
> **Proof:** By the remark above, we automatically have uniqueness if we can prove existence. Let $F(A, B)$ be the free $\mathbb{Z}$-module generated by $A \times B$. Let K be the subgroup of $F(A, B)$ generated by the elements:
>
> $$(a + a', b) - (a, b) - (a', b), \quad \text{for all } a, a' \in A \text{ and } b \in B,$$
>
> $$(a, b + b') - (a, b) - (a, b'), \quad \text{for all } a \in A \text{ and } b, b' \in B,$$
>
> $$(ar, b) - (a, rb), \quad \text{for all } a \in A \text{ and } b \in B \text{ and } r \in R.$$
>
> Let $A \otimes_R B = F(A, B)/K$.
>
> Let $m : A \times B \to A \otimes_R B$ defined by $(a, b) \mapsto a \otimes_R b :=$ the image of (a, b) in $F(A, B)/K$.

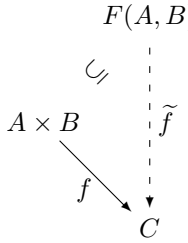
It remains to check that:

(1) m is a middle-linear map:

We need to verify that $f(a+a',b) = f(a,b)+f(a',b)$ and that $f(a,b+b') = f(a,b)+f(a,b')$ and that $f(ar,b) = f(a,rb)$. But, these are all imeediate from the definition of K as being generated by those particular elements.

(2) $m : A \times B \to A \otimes_R B$ is an initial object of $\mathscr{M}(A,B)$.

Let $f : A \times B \to C$ be a middle-linear map. We have to show that there exists a unique group homomorphism $\widetilde{f} : A \otimes_R B \to C$ such that $\widetilde{f}(a \otimes_R b) = f(a,b)$, for all $a \in A$ and $b \in B$. Consider the diagram:



By the universal property of $F(A,B)$, there exists $\hat{f} : F(A,B) \to C$ such that $\hat{f}(a,b) = f(a,b)$ for all $a \in A$ and $b \in B$. Now,

$$\begin{aligned}\hat{f}\left((a+a',b)-(a,b)-(a',b)\right)) &= \hat{f}(a+a',b) - \hat{f}(a,b) - \hat{f}(a',b)\\ &= f(a+a',b) - f(a,b) - f(a',b)\\ &= 0,\end{aligned}$$

since f is additive in A.

Similarly, you can check that

$$\hat{f}\left((a,b+b')-(a,b)-(a,b')\right)) = 0,$$

and

$$\hat{f}\left((ar,b)-(a,rb)\right) = 0.$$

Hence, $K \subseteq \operatorname{Ker}\hat{f}$. So, $\hat{f}$ induces a homomorphism $\hat{f} : F(A,B)/K \to C$ such that $\widetilde{f}(a,b) = \hat{f}(a,b) = f(a,b)$. Since the images of (a,b) for $a \in A$ and $b \in B$ generate $A \otimes_R B$, we have that $\widetilde{f}$ is the unique homomorphism with this property.

Hence, we have shown the existance of $A \otimes_R B$. $\square$

Example: Consider $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z})$. Since $a = 3a$ in this group, we have that

$$\begin{aligned}a \otimes_{\mathbb{Z}} b &= a \cdot 3 \otimes_{\mathbb{Z}} b\\ &= a \otimes_{\mathbb{Z}} 3 \cdot b\\ &= a \otimes_{\mathbb{Z}} 0\\ &= a \otimes_{\mathbb{Z}} 0 \cdot 0\\ &= a \cdot 0 \otimes_{\mathbb{Z}} 0\\ &= 0 \otimes_{Z} 0.\end{aligned}$$

Hence this group is trivial.

Example: Let A be a torsion abelian group. Consider $A \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $a \in A$ with $na = 0$. Then,

$$\begin{aligned} a \otimes_{\mathbb{Z}} r &= a \otimes_{\mathbb{Z}} n \cdot \frac{r}{n} \\ &= a \cdot n \otimes_{\mathbb{Z}} \frac{r}{n} \\ &= 0 \otimes_{\mathbb{Z}} \frac{r}{n} \\ &= 0 \otimes_{\mathbb{Z}} 0. \end{aligned}$$

Hence, A is trivial.

Example: Consider $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{R}$. This is very big.

Remark: Note that not every element of $A \otimes_R B$ can be written as $a \otimes_R b$. The tensor product is generated by those elements. So, to write an arbitrary element, it will be a finite sum of those elements.

Corollary IV.5.3: Consider the modules A_R, A'_R, ${}_RB$, ${}_RB'$. Let $f : A \to A'$ and $g : B \to B'$. Then, there exists a unique homomorphism of abelian groups:

$$(f \otimes_R g) : A \otimes_R B \to A' \otimes_R B'.$$

Proof: Consider the map $A \times B \to A' \otimes_R B'$ defined by $(a, b) \mapsto f(a) \otimes_R g(b)$. We check that this map is middle-linear. (Note the diagram: $A \times B \longrightarrow A' \times B' \xrightarrow{m} A' \otimes_R B'$.)

(1)
$$\begin{aligned} (a + a', b) &\mapsto f(a + a') \otimes_R g(b) \\ &= (f(a) + f(a')) \otimes_R g(b) \\ &= f(a) \otimes_R g(b) + f(a') \otimes_R g(b) \\ &= f(a, b) + f(a', b). \end{aligned}$$

(2)
$$\begin{aligned} (a, b + b') &\mapsto f(a) \otimes_R g(b + b') \\ &= f(a) \otimes_R (g(b) + g(b')) \\ &= f(a) \otimes_R g(b) + f(a) \otimes_R g(b') \\ &= f(a, b) + f(a, b'). \end{aligned}$$

(3)
$$\begin{aligned} (ar, b) &\mapsto f(ar) \otimes_R g(b) \\ &= f(a)r \otimes_R g(b) \\ &= f(a) \otimes_R rg(b) \\ &= f(a) \otimes_R g(rb) \\ &= f(a, rb). \end{aligned}$$

□

Proposition IV.5.4: (right exactness of $\otimes$) Let

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be an exact sequence of left R-modules. Let S be a right R-module. Then,

$$D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \longrightarrow 0$$

is exact.

Proof: First we show that $1_D \otimes g$ is surjective. Well, we know that g is surjective, and $D \otimes_R C$ is generated by elements $d \otimes c$. Given such an element, there exists $b \in B$ such that $g(b) = c$. Then, $(1_D \otimes g)(d \otimes b) = d \otimes c$. Hence, $1_D \otimes g$ is surjective.

Now we show in two steps that $\mathrm{Im}(1_D \otimes f) = \mathrm{Ker}(1_D \otimes g)$. First we show that $\subseteq$ inclusion. We know that $D \otimes A$ is generated by elements of the form $d \otimes a$ for $d \in D$ and $a \in A$. Well, $\mathrm{Im}(1 \otimes f)$ is generated by elements of the form $(1_D \otimes f)(d \otimes a) = d \otimes f(a)$. Now $(1 \otimes g)(d \otimes f(a)) = d \otimes g(f(a)) = 0$, since $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$. Thus $\mathrm{Im}(1_D \otimes f) \subseteq \mathrm{Ker}(1 \otimes g)$.

Now we show the reverse inclusion. Let $x \in \mathrm{Ker}(1 \otimes g) \subseteq D \otimes B$. We can write

$$x = \sum_i d_i \otimes b_i, \quad \text{for } d_i \in D \text{ and } b_i \in B.$$

Hence,

$$0 = (1 \otimes g)(x) = \sum_i d_i \otimes g(b_i) \in D \otimes C.$$

Recall that by assumption, $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

Let $\pi : D \otimes B \longrightarrow (D \otimes B)/\mathrm{Im}(1 \otimes f)$ be the canonical map. There is a homomorphism

$$(D \otimes B)/\mathrm{Im}(1 \otimes f) \xrightarrow{\alpha} D \otimes C$$

since $\mathrm{Im}(1 \otimes f) \leq \mathrm{Ker}(1 \otimes g)$.

Now, define $D \times C \longrightarrow (D \otimes B)/\mathrm{Im}(1 \otimes f)$ by $(d, c) \mapsto \pi(d \otimes b)$, where b is any element with $g(b) = c$.

We need to show that this is a well-defined middle linear map. Suppose $g(b) = g(b')$, then $b = b' + f(a)$ for some $a \in A$ by exactness of the sequence.

Observe that $d \otimes b = d \otimes (b' + f(a)) = (d \otimes b') + (d \otimes f(a))$. The last term is in $\mathrm{Im}(1 \otimes f)$, so we have the same element of $(D \otimes B)/\mathrm{Im}(1 \otimes f)$ and hence the map is well defined. $\square$

Tensor Products in Linear Algebra:

Let $R = F$ be a field. Then, all R-modules are vector spaces, and are all (R, R)-bimodules. Here, middle linear maps are equivalent to bilinear maps. So, if V, W are two vector spaces, then $V \otimes_F W$ is a vector space which is universal with respect to bilinear maps $V \times W \to U$ for some vector space U. So,

$$\{\text{Bilinear maps } V \times W \to U\} \quad \equiv \quad \{\text{Linear maps from } V \otimes_F W \to U\}$$

Theorem IV.5.7: If R is a ring with 1, and A_R and ${}_RB$ are modules, then

$$\begin{array}{ll} A \otimes_R R \cong A, & \text{as right } R\text{-modules, and} \\ R \otimes_R B \cong B, & \text{as left } R\text{-modules.} \end{array}$$

This is similar to the idea that $\mathrm{Hom}_R(R, A) \cong A$.

To prove this, use the map $A \times R \to A$ defined by $(a, r) \mapsto ar$ and the map $A \to A \otimes_R R$ defined by $a \mapsto a \otimes_R 1$.

Theorem IV.5.8: (Associativity of $\bigotimes$) Let R, S be rings (with 1). Let A_R, ${}_RB_S$ and ${}_SC$ be modules. Then,

$$(A \otimes_R B) \otimes_S C \cong A \otimes_R (B \otimes_S C).$$

(Not only are they isomorphic, they are *naturally isomorphic*, but we don't prove that here.)

Proof: It will not be feasible to try to explicity define a direct map because it is difficult to "write down" and element of either side. Instead, we will use the Universal Property of $\bigotimes$ and write down an intermediate map.

We know that $A \otimes_R B$ is generated by elements of the form $a \otimes_R b$, for $a \in A$ and $b \in B$.

Fix $c \in C$. Define $m_c : A \times B \to A \otimes_R (B \otimes_S C)$ by $m_c(a, b) = a \otimes_R (b \otimes_S c)$. Now, m_c is an R-middle linear map. So, m_c gives us a homomorphism $A \otimes_R B \to A \otimes_R (B \otimes_S C)$ defined by $a \otimes_R b \mapsto a \otimes_R (b \otimes_S c)$. Define m_c as such for all $c \in C$.

Now we define a map

$$(A \otimes_R B) \times C \longrightarrow A \otimes_R (B \otimes_S C)$$

$$(u, c) \longmapsto m_c(u)$$

First we check that this map is a well-defined S-middle-linear map. Then we get a homomorphism $(A \otimes_R B) \otimes_S C \longrightarrow A \otimes_R (B \otimes_S C)$. We see that this sends an element of the form $(a \otimes_R b) \otimes_S c \longmapsto a \otimes_R (b \otimes_S c)$.

Next we define a homomorphism in the other direction, using functions m_a defined analogously, to get a homomorphism in the other direction. We check that the composition of these two homomorphisms in either direction gives us the identity, and hence they are inverse maps and thus bijections. Therefore, each is an isomorphism. □

Remark: If we have ${}_TA_R$ and ${}_RB_S$, then $A \otimes_R B$ is a (T, S)-bimodule. I.e., ${}_T(A \otimes_R B)_S$.

If R, S rings, then consider the map $R \xrightarrow{f} S$. If we have a module ${}_SM$, we can make M into an R-module by $r \cdot m := f(r)m$, which is called the pullback.

We can also get S-modules from R-modules. If we start with A_R and ${}_RS_s$, with the left R-module structure on S given by f, then $A \otimes_R S$ is a right S-module. This is called the scalar extension of A along f.

With a map $\mathbb{Z} \xrightarrow{f} \mathbb{Z}/p\mathbb{Z}$ and M and abelian group, we can show that $M \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z}) = M/pM$.

Example:

$$(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}, \text{ where } d = \gcd(m, n).$$

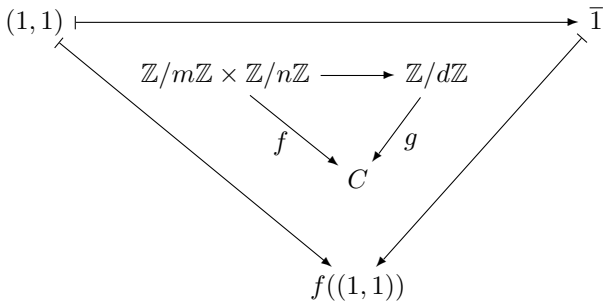
To prove, use the Universal Property of $\bigotimes$. Consider a map $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/d\mathbb{Z}$, defined by $(a, b) \mapsto \overline{a}\overline{b}$, where $\overline{a} \equiv a \bmod d$ and $\overline{b} \equiv b \bmod d$. This is obviously middle-linear (in a $\mathbb{Z}$-module, bilinear just means additive in each variable, which is true here). Now suppose $f : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to C$ is a middle-linear map (i.e., biadditive). Now:

(1) $f((0, b)) = f((a, 0)) = 0$, for all $a \in \mathbb{Z}/m\mathbb{Z}$ and $b \in \mathbb{Z}/n\mathbb{Z}$.

(2) f is completely determined by $f((1,1))$. Clearly, $f((a,b)) = f((\hat{a}\cdot 1, 1\cdot \hat{b})) = \hat{a}\hat{b}\cdot f((1,1))$, where $\widehat{a}$ mod $m = a$ and $\widehat{b}$ mod $m = b$.

(3) $mf((1,1)) = f((m,1)) = f((0,1)) = 0$ and $nf((1,1)) = f((1,n)) = f((1,0)) = 0$. So, $df((1,1)) = 0$. So, there exists a homomorphism $g : \mathbb{Z}/d\mathbb{Z} \to C$ defined by $\overline{1} \mapsto f((1,1))$.

Now we have the diagram:



Hence $\mathbb{Z}/d\mathbb{Z}$ has the defining property of $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$.

Example: $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q} \cong \mathbb{Q}$ by a theorem that $R \otimes_R A \cong A$.

More surprisingly $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$. To see this informally, observe that

$$\frac{p}{q} \otimes \frac{r}{s} = \frac{pr}{q} \otimes \frac{1}{s} = \frac{prs}{qs} \otimes \frac{1}{s} = \frac{pr}{qs} \otimes \frac{s}{s} = \frac{pr}{qs} \otimes 1.$$

Theorem IV.5.9: Let R be a ring, let A and $\{A_i\}_{i\in I}$ be right R-modules, and let B and $\{B_j\}_{j\in J}$ be left R-modules. Then,

$$\left(\sum_{i\in I} A_i\right) \otimes_R B \cong \sum_{i\in I} (A_i \otimes_R B)$$

and

$$A \otimes_R \left(\sum_{j\in J} B_j\right) \cong \sum_{j\in J} (A \otimes_R B_j).$$

Proof: To prove, you must use the Universal Property of Coproducts. With the first one, define a map from the left-hand side to right-hand side using the universal properties, and do the same thing in the other direction, and show that the two maps are inverse maps, hence isomorphisms. To define the first map, we need a middle-linear map from the $\sum A_i \times B$ to $\sum(A_i \otimes B)$. To do this, we start with maps for each A_i into $\sum(A_i \otimes B)$ and work up from there. For the reverse map, we start with maps from $A_i \otimes B$ to the left-hand side and then work up from there.

Theorem IV.5.10: (Adjoint Associativity) Let R ans S be rings. Consider A_R, ${}_RB_S$, and C_S. Then there is an isomorphism of abelian groups

$$\alpha : \mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$$

such that if $f \in \mathrm{Hom}_S(A \otimes_R B, C)$, then $[(\alpha f)(a)](b) = f(a \otimes b)$.

In particular, applied to the case where $R = S = F$ for a field F and letting $C = F$, we have that

$$(A \otimes B)^* \cong \mathrm{Hom}_R(A, B^*).$$

Proof: We need to show that $(\alpha f)(a) \in \mathrm{Hom}_S(B, C)$. Then we show that $(\alpha f) \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$. Then we show that α is a homomorphism.

First, (we show only the module property, we skip the abelian group (additivity) property)

$$\begin{aligned}(\alpha f)(a)(bs) &= f(a \otimes bs)\\ &= f(a \otimes b)s\\ &= [(\alpha f)(a)(b)]s.\end{aligned}$$

Hence $(\alpha f)(a) \in \mathrm{Hom}_S(B, C)$.

Next,

$$\begin{aligned}(\alpha f)(ar)(b) &= f(ar \otimes_R b)\\ &= f(a \otimes_R rb)\\ &= (\alpha f)(a)(rb)\\ &= [[(\alpha f)(a)]r](b).\end{aligned}$$

Hence $(\alpha f)(ar) = [(\alpha f)(a)]r$.

Now let $\beta : \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \to \mathrm{Hom}_S(A \otimes_R B, C)$. For $g \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C))$, we want to define $(\beta g) \in \mathrm{Hom}_S(A \otimes B, C)$.

Define $m_g : A \times B \to C$ by $(a, b) \mapsto g(a)(b)$. This is a middle linear map, and so it defines $\mu_g : A \otimes_R B \to C$. Set $\beta(g) = \mu_g \in \mathrm{Hom}_S(A \otimes_R B, C)$.

We have defined

$$\beta : \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \to \mathrm{Hom}_S(A \otimes_R B, C)$$

We have shown that β is a homomorphism. Finally, we need to check that α and β are inverses.

$$\begin{aligned}(\alpha(\mu_g)(a)(b) &= \mu_g(a \otimes b)\\ &= g(a)(b).\end{aligned}$$

Hence $\alpha(\mu_g) = g$, i.e., $\alpha \circ \beta = \mathrm{Id}$. Similarly, we can show the other direction. Therefore α is an isomorphism. □

Theorem IV.5.11: Let R be a ring with 1. If A is a unital right R-module and F is a free left module with basis Y, then every element u of $A \otimes_R F$ can be written uniquely in the form

$$u = \sum_{i=1}(a_i \otimes y_i),$$

where each $y_i \in Y$ are distinct.

Proof: For $y \in Y$, we have $Ry \cong R$ as left R-modules, and $F = \sum_{y \in Y} R_y$. So,

$$A \otimes_R F \cong A \otimes_R \left(\sum_{y \in Y} R_y \right) \cong \sum_{y \in Y} (A \otimes_R R_y).$$

Since $Ry \cong R$ as left R-modules, we have

$$A \otimes_R y \cong A \otimes_R \cong A.$$

Hence,

$$\sum_{y \in Y} (A \otimes_R R_y) \cong \sum_{y \in Y} A,$$

where A is a copy for each $y \in Y$. □

Corollary IV.5.12: Suppose R has a 1. If A_R is a free unital right module with basis X, and ${}_RB$ is a free left module with basis Y, then $A \otimes_R B$ is a free (right) R module with basis $W = \{x \otimes y \mid x \in X,\ y \in Y\}$ of cardinality $|X||Y|$. Note that since A and B are free modules, they are really both left and right modules, and the tensor product can be considered as both a left and right module.

Corollary IV.5.13: Let S be a ring with 1 and R a subring with $1_S \in R$. If F is a free left R-module then $S \otimes_R F$ is a free left S-module with basis $\{a \otimes_R x \mid x \in X\}$.

1.3.6 Section IV.7 - Algebras

Definition: Let K be a commutative ring with 1. A $\underline{K\text{-algebra}}$ is a ring A such that:

(1) $(A, +)$ is a unital left K-module.

(2) $k(ab) = (ka)b = a(kb)$, for all $k \in K$ and $a, b \in A$.

Note 1: In some textbooks, an algebra is defined (sometimes implicitly) to require a 1, but not here.
Note 2: Some people define way more general structures that only satisfy the first condition, and they call these "algebras". To distinguish, the algebras defined above are sometimes called "associative algebras".

Example: Every ring is a $\mathbb{Z}$-algebra.

Example: If K is commutative with 1, then $K[x_1, \ldots, x_n]$, $K[[x]]$, etc are all K-algebras.

Example: If V is a vector space over F, then $\mathrm{End}_F(V)$ is an F-algebra.

Example: If A is a ring with 1 and K is a subring of $Z(A)$ containing 1_A, then A is a K-algebra. In particular, every commutative ring with 1 is an algebra over itself.

Theorem IV.7.2: Let K be a commutative ring with 1, and A a left unital K-module. Then, A is a K-algebra if and only if there exists a K-module homomorphism

$$\pi : A \otimes_K A \to A$$

such that we have the commutative diagram:

$$\begin{array}{ccc} a \otimes b \otimes c & \longmapsto & (ab) \otimes c \\ \downarrow & & \downarrow \\ A \otimes_K A \otimes_K A & \xrightarrow{\pi \otimes 1_A} & A \otimes_K A \\ \downarrow{\scriptstyle 1 \otimes \pi} & & \downarrow{\scriptstyle \pi} \\ A \otimes_K A & \xrightarrow{\pi} & A \\ \downarrow & & \downarrow \\ a \otimes (bc) & \longmapsto & a(bc) \end{array}$$

Moreover, A has a 1 if and only if there exists a K-module homomorphism $I : K \to A$ such that the following diagram commutes:

$$\begin{array}{ccccc} K \otimes_K A & \xrightarrow{\xi} & A & \xleftarrow{\theta} & A \otimes K \\ \downarrow{\scriptstyle I \otimes 1_A} & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle 1_A \otimes I} \\ A \otimes_K A & \xrightarrow{\pi} & A & \xleftarrow{\pi} & A \otimes_K A \end{array}$$

Note that ξ and θ are the isomorphism of **Theorem 5.7**.

Theorem IV.7.4: If A and B are K-algebras, then $A \otimes_K B$ is a K-algebra with multiplication:

$$(A \otimes_K B) \otimes_K (A \otimes_K B) \to A \otimes_K B.$$

We also have an isomorphism:

$$\alpha : B \otimes A \longrightarrow A \otimes B,$$

$$\alpha : b \otimes a \longmapsto a \otimes b.$$

Proof: Let π_A be the product map on A and let π_B be the product map on B. We'd like to be able to send $(a \otimes b) \otimes (a' \otimes b')$ to $aa' \otimes bb'$, but we need to do this in terms of the product maps. By associativity, we can redefine the multiplication map as

$$A \otimes (B \otimes A) \otimes B \to A \otimes B$$

by some map θ.

Under the map $1 \otimes \alpha \otimes 1$, we can map $A \otimes (B \otimes A) \otimes B$ to $A \otimes (A \otimes B) \otimes B$. Lastly, we can reassociate via γ to $(A \otimes A) \otimes (B \otimes B)$. Lastly, we use the product maps π_A and π_B to send $A \otimes A \to A$ and $B \otimes B \to B$. Hence, the multiplication map is:

$$\pi_b \circ \pi_a \circ \gamma \circ (1 \otimes \alpha \otimes 1) \circ \theta.$$

Examples:

(1) $M_n(F) \otimes_F A \cong M_n(A)$. Special case: $M_n(F) \otimes_F M_m(F) \cong M_{mn}(F)$.

(2) Hamilton Quaternions: $\mathbb{H} := \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. The center of $\mathbb{H}$ is the set where $b = c = d = 0$, i.e., $Z(\mathbb{H}) = \mathbb{R}$. Now, $\mathbb{H} \otimes_R \mathbb{C} \cong M_n(\mathbb{C})$. Also, $\mathbb{H} \otimes_R \mathbb{H} \cong M_4(\mathbb{R})$.

1.4 Chapter III - Rings

1.4.1 Section III.4 - Rings of Quotients and Localization

Definition: Let R be a commutative ring (not necessarily with 1). A nonempty set $S \subseteq R$ is multiplicative if for all $s_1, s_2 \in S$ we have $s_1 s_2 \in S$, i.e., S is closed under multiplication.

Theorem III.4.2: Consider the relation on $R \times S$ given by

$$(r, s) \sim (r', s') \text{ if and only if } \exists s'' \in S : \quad s''(rs' - r's) = 0.$$

This is an equivalence relation. Furthermore, if R has no zero divisors and $0 \notin S$, then $(r, s) \sim (r', s')$ if and only if $rs' = r's = 0$.

Let $S^{-1}R$ denote the set of equivalence classes and write $\frac{r}{s}$ for the class of (r, s).

(i) $\frac{r}{s} = \frac{r'}{s'}$ if and only if there exists s'' such that $s''(r's - rs') = 0$.

(ii) $\frac{tr}{ts} = \frac{r}{s}$ for all $t \in S$.

(iii) If $0 \in S$, then $S^{-1}R$ has just one class.

Theorem III.4.3:

(i) $S^{-1}R$ is a ring with addition and multiplication defined as follows.

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + r's}{ss'}.$$

$$\frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

(ii) If R is a nonzero ring with no zero divisors, and $0 \notin S$, then $S^{-1}R$ is an integral domain.

(iii) If R is a nonzero ring with no zero divisors, and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field.

Proof that the ring addition is well defined in $S^{-1}R$:

Suppose $\frac{r}{s} = \frac{r_1}{s_1}$ and $\frac{r'}{s'} = \frac{r'_1}{s'_1}$. We want to check that $\frac{rs' + r's}{ss'} = \frac{r_1 s'_1 + r'_1 s_1}{s_1 s'_1}$.

By the first equality, there exists $t \in S$ such that $t(rs_1 - r_1 s) = 0$ and by the second equality, there exists $t' \in S$ such that $t'(r's'_1 - r'_1 s') = 0$.

Multiplying the first equation by $t's'_1 s'$, we have

$$t's'_1 s' trs_1 - t's'_1 s' tr_1 s = 0.$$

Multiplying the second equation by $ts_1 s$, we have

$$ts_1 st'r's'_1 - ts_1 st'r'_1 s' = 0.$$

Now, we add the two equations together:

$$tt's'_1 s_1(rs' + sr') = tt'ss'(r_1 s'_1 + r'_1 s_1).$$

Hence

$$tt'((s_1s')(rs' + sr') - (ss')(r_1s_1' + r_1's_1)) = 0.$$

This tells us that the ring addition is well defined. □

Definition: $S^{-1}R$ is called the localization of R with respect to S, or the ring of quotients of R with respect to S. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is called the field of fractions of R. If the set of non-zero-divisors is not empty, then taking S to be this set, we call $S^{-1}R$ the full ring of quotients of R.

Theorem III.4.4: Let S be a multiplicative set in R.

(i) The map $\varphi_s : R \to S^{-1}R$ defined by $r \mapsto \frac{rs}{s}$, (for any $s \in S$) is a (well-defined) homomorphism of rings.

(ii) If $0 \notin S$ and S has no zero divisors, then φ_s is a monomorphism.

(iii) If R has a 1 and S consists of units, then φ_s is an isomorphism.

Some sketches of parts of proof:
Let $r \in \operatorname{Ker} \varphi_s$. Then,

$$\frac{rs}{s} = \frac{0s}{s}$$

and so there exists $t \in S$ such that

$$t(rs^2 - 0s^2) = 0$$

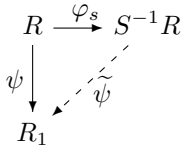
Thus, if $ts^2 \neq 0$, we have that $r = 0$.

Recall: Let R be a commutative ring. Let S be a multiplicative set. Let $\varphi_s : R \to S^{-1}R$ be defined by $r \mapsto \frac{rs}{s}$. This is a canonical map because it's independent of the choice of s.

Theorem: (Universal Mapping Property of φ_s)

φ_s has the following Universal Mapping Property:

If $\psi : R \to R_1$ is any ring homomorphism such that $\psi(s)$ is a unit for all $s \in S$, then there exists a unique homomorphism $\widetilde{\psi} : S^{-1}R \to R_1$ such that the diagram below commutes:



Proof: Define $\widetilde{\psi}\left(\frac{r}{s}\right) := \psi(r)\psi(s)^{-1}$, and check that this map is well defined as follows:

Suppose $\frac{r}{s} = \frac{r_1}{s_1}$. Then, there exists $t \in S$ such that $t(s_1r - r_1s) = 0$. Then,

$$\psi(t)(\psi(s_1)\psi(r) - \psi(r_1)\psi(s) = 0.$$

But, $\psi(t)$ is a unit. So, we have that $\psi(s_1)\psi(r) = \psi(r_1)\psi(s)$. Since $\psi(s)$ and $\psi(s_1)$ are units, we get that $\psi(r)\psi(s)^{-1} = \psi(r_1)\psi(s_1)^{-1}$, and so $\frac{r}{s} = \frac{r_1}{s_1}$.

Need to check that it is a homomorphism. This is routine. □

Remark: A special case from this is a theorem we used last year and earlier this year: If you have a homomorphism from an integral domain into a field, you can extend it to a homomorphism from the quotient field of the integral domain to the field.

Next we consider how the ideals of R are related to the ideals of $S^{-1}R$.

If I is an ideal of R, then let $S^{-1}I = \{\frac{r}{s} \mid r \in I,\ s \in S\}$. Then, $S^{-1}I$ is an ideal of $S^{-1}R$. To see this, pick $\frac{a}{s} \in S^{-1}I$, with $a \in I$ and $s \in S$. Let $\frac{r}{s'} \in S^{-1}R$. Then, $ra \in I$, so $\frac{ra}{s's} \in S^{-1}I$. Similarly, $\frac{a}{s} - \frac{b}{s'} = \frac{s'a-sb}{ss'} \in S^{-1}I$, and so it's closed under subtraction. Therefore, it's an ideal.

If J is an ideal of $S^{-1}R$, then let $\varphi_s^{-1}(J)$ denote the full preimage in R of J. This is an ideal of R.

Theorem III.4.7: If I and J are ideals of R, then:

(a) $S^{-1}(I+J) = S^{-1}I + S^{-1}J$

(b) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$

(c) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$

Proof of (a): Let $a \in I$ and $b \in J$. Let $\frac{a+b}{s} \in S^{-1}(I+J)$. But, $\frac{a+b}{s} = \frac{a}{s} + \frac{b}{s}$. Thus, $S^{-1}(I+J) \subseteq S^{-1}I + S^{-1}J$. Now consider $\frac{a}{s} \in S^{-1}I$ and $\frac{b}{s'} \in S^{-1}J$. Note that $\frac{a}{s} + \frac{b}{s'} = \frac{as'+bs}{ss'} \in S^{-1}(I+J)$. □

Theorem III.4.8: Let I be an ideal of R. Then, $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \emptyset$.

Lemma III.4.9:

(i) $I \subseteq \varphi_s^{-1}(S^{-1}I)$

(ii) If $I = \varphi_s^{-1}(J)$ to some ideal J of $S^{-1}R$, then $S^{-1}I = J$. Hence ever ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.

(iii) If P is a prime ideal of R and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal of $S^{-1}R$ and $\varphi_s^{-1}(S^{-1}P) = P$.

Proof: The proof of (i) is trivial.

For (ii): let $a \in I$ and $s \in S$. Then, $\varphi_s(a) \in J$. So $\frac{as}{s} \in J$. Then, $\frac{a}{s} = \frac{as}{s} \cdot \frac{s}{s^2} \in J$. Hence, $S^{-1}I \subseteq J$. Now let $\frac{r}{s} \in J$. Then, $\frac{rs}{s} \in J$, and $\frac{rs}{s} = \varphi_s(r)$. Therefore, $r \in \varphi_s^{-1}(J)$ and $\frac{r}{s} \in S^{-1}(\varphi_s^{-1}(J))$, and this proves (ii).

For (iii): Since $S \cap P = \emptyset$, then $S^{-1}P$ is a proper ideal. Let $\frac{a}{s}, \frac{b}{s'} \in S^{-1}R$ and suppose $\frac{ab}{ss'} \in S^{-1}P$. So, there exists $p \in P$ such that $\frac{ab}{ss'} = \frac{p}{t}$. Then, there exists t' such that $t'(abt - pss') = 0$. Hence, $abtt' = pss't' \in P$. So, $abtt' \in P$. Since $t, t' \in S$, they cannot be in the prime ideal. Hence either $a \in P$ or $b \in P$, and so either $\frac{a}{s}$ or $\frac{b}{s'}$ is in $S^{-1}P$. It remains to show that $\varphi_s^{-1}(S^{-1}P) = P$.

Suppose that $r \in R$, and $\varphi_s(r) \in S^{-1}(P)$. Then, $\frac{rs}{s} = \frac{p}{t}$ for some $s, t \in S$ and $p \in P$. Thus, there exists $t' \in S$ such that $(rst - ps)t' = 0$, and so $rstt' = pst' \in P$. Since $s, t, t' \in S$, they're not in P. So, $r \in P$. □

Theorem III.4.11: There is a one-to-one correspondence:

$$\left\{ \text{ prime ideals } P \text{ of } R \text{ such that } P \cap S = \emptyset \right\} \underset{\varphi_S^{-1}(J) \longleftarrow\!\shortmid\ J}{\overset{P \longmapsto S^{-1}P}{\rightleftarrows}} \left\{ \text{ prime ideals of } S^{-1}R. \right\}$$

Proof: The only thing we haven't shown yet is that for J a prime ideal of $S^{-1}R$, the ideal $\varphi_S^{-1}(J)$ is prime. Let $a, b \in R$ with $ab \in \varphi_S^{-1}(J)$. Then, $\varphi_S(a)\varphi_S(b) = \varphi_S(ab) \in J$ and J is prime. So, either $\varphi_S(a) \in J$ or $\varphi_S(b) \in J$. Hence, either $a \in \varphi_S^{-1}(J)$ or $b \in \varphi_S^{-1}(J)$. □

Special Case: Let P be a prime ideal of R and let $S = R \setminus P$. Then, S is a multiplicative set. Here, tthe ring $S^{-1}R$ is denoted by R_P and called the localization of R at the prime ideal P. By the theorem, the prime ideals of R_P are in one-to-one correspondence with the prime ideals of R contained in P. Hence P_P is the unique maximal ideal of R_P.

Definition: A local ring is a commutative ring with identity which has a unique maximal ideal.

Theorem III.4.14: Let R be a commutative ring with identity. The following are equivalent:

(i) R is a local ring.

(ii) All nonunits of R are contained in some proper ideal M.

(iii) The nonunits of R form an ideal.

Example: Let $R = \mathbb{Z}$ and p primes. Then, $\mathbb{Z}_{(p)} = \{r/s \in \mathbb{Q} \mid p \nmid s\}$.

Example: Consider the ring $K[x_1, \ldots, x_n]$ with maximal ideal $M = (x_1, \ldots, x_n)$. Then,

$$K[x_1, \ldots, x_n]_M = \{f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n) \in K(x_1, \ldots, x_n) \mid g(0, \ldots, 0) \neq 0\}.$$

1.5 Chapter VIII - Commutative Rings and Modules

1.5.1 Section VIII.1 - Chain Conditions

Definition: A module satisfies the ascending chain condition (abbreviated ACC) if for every chain

$$A_1 \subset A_2 \subset \cdots$$

of submodules there exists n such that $A_i = A_n$ for all $i \geq n$, i.e. the chain stabilizes. Note that we are checking only countable chains. These modules are called Noetherian modules.

Definition: A module satisfies the descending chain condition (abbreviated DCC) if for every chain

$$B_1 \supset B_2 \supset \cdots$$

of submodules there exists n such that $B_i = B_m$ for all $i \geq m$. These modules are called Artinian modules.

Remark: Though these conditions appear symmetrical, they are not. In fact, the descending chain condition is in some ways much more restrictive than the ascending chain condition. For example, the module $\mathbb{Z}$ satisfies ACC but not DCC.

Definition: If R is a ring, then R is called left Noetherian/Artinian if and only if R as a left module over itself is Noetherian/Artinian. Similarly for right Noetherian/Artinian.

Definition: A module satisfies the maximum (resp. minimum) condition if every nonempty set of submodules has a maximal (resp. minimal) element, with respect to inclusion.

Theorem VIII.1.4: Let A be a module. Then A satisfies ACC if and only if A satisfies the maximum condition. Additionally, A satisfies DCC if and only if A satisfies the minimal condition.

> **Proof:** Let $\mathscr{S}$ be a nonempty set of submodule of A, and suppose ACC holds for A. Let $A_1 \in \mathscr{S}$. If A_1 is maximal then we're done. Otherwise, there exists $A_2 \in \mathscr{S}$ with $A_1 \subsetneq A_2$. If A_2 is maximal then we're done. Otherwise, there exists $A_3 \in \mathscr{S}$ such that $A_1 \subsetneq A_2 \subsetneq A_3$. Repeat this process. If we don't find a maximal element then we have an infinite ascending chain, which violates ACC. So the maximum condition holds.
>
> Now let A satisfy the maximum condition. Consider the chain
>
> $$A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$$
>
> of submodules. Then, by the maximum condition, the set $\{A_i \mid i \in \mathbb{N}\}$ has a maximal element, and so the chain stabilizes. Thus ACC holds.
>
> The proof for the equivalence of DCC and the minimum condition is similar. $\square$

Theorem VIII.1.5: Consider the short exact sequence of modules

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

Then, B satisfies ACC (resp. DCC) if and only if A and C satisfy ACC (resp. DCC).

Proof: See Hungerford.

Corollary VIII.1.7: If $A_1, \ldots, A_n$ are modules, then $\bigoplus_{i=1}^{n} A_i$ satisfies ACC/DCC if and only if each A_i does. This follows from induction using the previous theorem.

Theorem VIII.1.8: If R is a left (resp. right) Noetherian (resp. Artinian) ring with 1, then every finitely generated left (resp. right) R-module A satisfies ACC (resp. DCC).

Theorem VIII.1.9: A satisfies ACC if and only if every submodule of A is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal is finitely generated. (Recall that a finitely generated ring can have non-finitely-generated ideals.) There is no analogous statement for DCC.

Proof:
($\Longrightarrow$):

Let A satisfy ACC. Fix a submodule C of A. Consider the set of all finitely generated submodules of C. By the maximal condition (which is equivalent to ACC), there is a maximal finitely generated submodule B of A, i.e. any submodule of C that properly contains B is not finitely generated. Let $c \in C$. Then, the submodule generated by B and c is finitely generated. So, by maximality $c \in B$, and hence $B = C$ so C is finitely generated. Since C was arbitrary, all submodules of A are finitely generated. $\square$

($\Longleftarrow$):

Let every submodule of A be finitely generated. Let $A_1 \subseteq A_2 \subseteq \cdots$ be a chain of submodules of A. Then, $\bigcup A_i$ is a submodule A and hence also finitely generated by some elements $a_1, \ldots, a_n$. For each a_i, there exists some j_i with $a_i \in A_{j_i}$. Then, there exists $k := \max\{j_i\}$ such that $a_i \in A_k$ for all i, and so $\bigcup A_i = A_k$. Thus, $A_\ell = A_k$ for all $\ell \geq k$, i.e. the chain stabilizes. Since the chain was arbitrary, A satisfies ACC. $\square$

The second statement is an application of the first, in the case where R is an R-module over itself.

Normal Series (modern terminology: filtration)

Definition: Let A be a module. A normal series is a sequence

$$0 \subseteq A_n \subseteq A_{n-1} \subseteq \cdots \subseteq A_1 \subseteq A_0 = A.$$

The quotients A_i/A_{i+1} are called the factors. The length is the number of proper inclusions (i.e., the number of nontrivial factors). From a given normal series we obtain a refinement by adding in terms to the series. This refinement is a proper refinement if it increases the length.

Definition: We say that two normal series are equivalent if there is a one-to-one correspondence between the nontrivial factors such that corresponding factors are isomorphic modules.

Definition: A composition series for A is a normal series in which each factor A_i/A_{i+1} is a nonzero module with no nonzero proper submodules.

Theorem VIII.1.10: Any two normal series of a module A have refinements that are equivalent. Any two composition series are equivalent.

Theorem VIII.1.11: A module A has a composition series if and only if A satisfies both ACC and DCC.

Proof:
($\Longrightarrow$):

Let A have a composition series, with some finite length n. If ACC or DCC fails, then we can make a proper refinement of length $n+1$. Since any two normal series have refinements that are isomorphic, and any refinement of a composition series is not proper, this is a contradiction (the refinements of the composition series of length n all have length n, and the refinements of the normal series of length $n+1$ all have length $\geq n+1$, so the two refinements can never be equivalent). Thus, both ACC and DCC hold. $\square$

($\Longleftarrow$):

See Hungerford.

Example: Let D be a division ring. Then, show that $M_n(D)$ satisfies both ACC and DCC (on left ideals). Define

$$e_i := \begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix}$$

with a 1 in the (i,i) entry. See book for rest.

1.5.2 Section VIII.2 - Prime and Primary Ideals

In this section, unless stated otherwise, all rings are commutative and have an identity.

Definition: An ideal P of a ring is prime if $ab \in P$ implies either $a \in P$ or $b \in P$.

Definition: An ideal Q of a ring is primary if $ab \in Q$ and $a \notin Q$ then there exists $k \in \mathbb{N}$ such that $b^k \in Q$.

Example: In $\mathbb{Z}$, prime ideals are the ideals (p) where p is prime or zero. The ideal (p^n) for $n \geq 2$ is a primary ideal which is not a prime ideal. The ideal $(2^3 3^2)$ is neither prime nor primary.

Remark: If R is a Principal Ideal Domain (hence a Unique Factorization Domain), then the primary ideals are ideals (π^n) for $n \in \mathbb{N}$ and π prime. We can state the Unique Factorization Property in terms of the primary ideals: Let $a = \pi_1^{e_1} \cdots \pi_r^{e_r}$ for π_i non-associate primes. Then, we can write

$$(a) = (\pi_1^{e_1}) \cdots (\pi_r^{e_r}) = (\pi_1^{e_1}) \cap \cdots \cap (\pi_r^{e_r}).$$

Definition: The set of prime ideals of a commutative ring A is called the spectrum of A, denoted $\text{spec}(A)$. We say a set $S \subseteq \text{spec}(A)$ is closed if and only if there exists an ideal I such that

$$S = V(I) := \{p \in \text{spec}(A) \mid p \supseteq I\}.$$

We get a topology on A, called the Zariski topology.

Theorem VIII.2.2: Let S be a multiplicative subset of R and I an ideal such that $S \cap I = \emptyset$. Then, there exists an ideal $P \supseteq I$ which is maximal relative to being disjoint from S. Moreover P is prime.

Theorem VIII.2.3: Let K be a subring of a commutative ring R and suppose $P_1, \ldots, P_n$ are prime ideals of R such that $K \subset P_1 \cup P_2 \cup \cdots \cup P_n$. Then, there exists i such that $K \subseteq P_i$.

Proof: We can assume that $n \geq 2$ and for all i, $K \not\subseteq \bigcup_{\substack{j=1 \\ j \neq i}}^{n} P_j$.

Then, for each i, there exists a_i such that $a_i \in K \smallsetminus \bigcup_{\substack{j=1 \\ j \neq i}}^{n} P_j$. So, $a_i \in P_i$.

Now, $K \ni a_1 + (a_2 \cdots a_n) \in \bigcup_{i=1}^{n} P_i$. If $a_1 + (a_2 \cdots a_n) \in P_1$, then $a_2 \cdots a_n \in P_1$, and hence some $a_j \in P_1$ for $j \geq 2$, which is a contradiction. Thus, $a_1 + (a_2 \cdots a_n) \in P_j$ for some $j \geq 2$, but this implies $a_1 \in P_j$, also a contradiction. $\square$

Proposition VIII.2.4: Let R be a commutative ring with identity and P an ideal which is maximal in the set of all ideals of R which are not finitely generated. Then P is prime.

Proof: Suppose toward a contradiction that nonzero $a, b \in R$, $ab \in P$, but $a \notin P$ and $b \notin P$. We consider the ideals $P + (a)$ and $P + (b)$, which are ideals properly containing P, and so are finitely generated by the maximality of P.

We can write $P + (a) = \{p_1 + r_1 a, \ldots, p_n + r_n a\}$ for $p_i \in P$ and $r_i \in R$. Also, $P + (b) = \{p'_1 + r'_1 b, \ldots, p'_m + r'_m b\}$, for $p'_i \in P$ and $r'_i \in R$.

Now let $J := \{r \in R \mid ra \in P\}$. J Is an ideal, and

$$(p_i' + r_i'b)(a) = \underbrace{p_i'a}_{\in P} + \underbrace{r_i'ba}_{\in P}$$

so $(p_i' + r_i'b) \in J$, thus $P + (b) \subseteq J$. By the maximality of P, J is finitely generated.

Suppose $J = (j_1, \ldots, j_k)$. Let $x \in P$. Then, $x \in P + (a)$, and so we can write

$$x = \sum_{i=1}^{n} s_i(p_i + r_i a) \text{ for some } s_i \in R.$$

Now,

$$\left(\sum s_i r_i\right) a = x - \sum s_i p_i \in P$$

and so

$$\sum_{i=1}^{n} s_i r_i \in J.$$

Thus we can write

$$\sum_{i=1}^{n} s_i r_i = \sum_{\ell=1}^{k} t_\ell j_\ell.$$

Hence,

$$x = \sum s_i p_i + \sum t_\ell j_\ell a,$$

i.e.,

$$x \in (p_1, \ldots, p_n, j_1 a, \ldots, j_k a).$$

Since x was arbitrary and $p_1, \ldots, p_n, j_1 a, \ldots, j_k a$ are independent of x, this shows that

$$P = (p_1, \ldots, p_n, j_1 a, \ldots, j_k a),$$

which is a contradiction. □

Definition: Let I be an ideal in a commutative ring R. The radical of I, denoted $\text{rad}(I)$ is the intersection of all prime ideals containing I. If $I = (0)$, then is radical is called the nilradical.

Theorem VIII.2.6: Let I be an ideal. Then $\text{rad}(I) = \{x \in \mathbb{R} \mid \exists n \in \mathbb{N} : \ x^n \in I\}$.

Proof: First we show $\supseteq$. Suppose $x^n \in \bigcap_{P \supseteq I} P$. Then, $x^n \in P$ for all prime ideals P. Since each P is prime, $x \in P$ for all prime ideals P. Thus, x is in the intersection of all prime ideals.

Next we show $\subseteq$. Suppose $x \in \bigcap_{P \supseteq I} P$ and suppose for a contradiction that $x^n \notin I$ for all n¿ Then, $S = \{x^n \mid n \in \mathbb{N}\}$ is a multiplicative set such that $S \cap I = \emptyset$. By a theorem above (pg. 5?), we have that there exists a prime ideal P' such that $P' \cap S = \emptyset$, which is a contradiction since x is in all prime ideals. □

Theorem VIII.2.7: If $I_1, \ldots, I_n$ are ideals of R, then

(i) $\text{rad}(\text{rad}(I)) = \text{rad}(I)$,

(ii) $\text{rad}(I_1 I_2 \cdots I_n) = \text{rad}\left(\bigcap (I_j)\right) = \bigcap (\text{rad}(I_j))$,

(iii) $\text{rad}(I^m) = \text{rad}(I)$.

Remark: Observe that powers of prime ideals are primary ideals, but primary ideals may not be powers of prime ideals. Additionally, powers of prime ideals may not be primary.

Example: Let $R = F[x, y]$ for a field F. Let $P := (x, y)$. Then P is a prime ideal. Now, $P^2 = (x^2, xy, y^2)$. Consider the ideal between them $Q := (x^2, y)$, so that $P \supsetneqq Q \supsetneqq P^2$. We claim that Q is a primary ideal but not the power of a prime ideal. If $Q = P_1^r$, then $Q \subseteq P_1$. Hence the only possibility for P_1 is P, but this is not possible.

Example: Consider $\mathbb{C}[x, y, z]/(xy - z^2)$ and the prime ideal $P = (x, z)$ (which is prime because $R/P \cong \mathbb{C}[y]$, which is an integral domain). Now, $P^2 = (x^2, xz, z^2) = (x^2, xz, xy)$. Note that $z^2 = xy$ because we are in the quotient by the polynomial $xy - z^2$. Now, $xy \in P^2$, but $x \notin P^2$ and $y^n \notin P^2$ for all n. Thus, P^2 is not primary.

Theorem VIII.2.9: If Q is primary, then $\text{rad}(Q)$ is prime.

> **Proof:** Suppose that $ab \in \text{rad}(Q)$ and $a \notin \text{rad}(Q)$. Then, there exists n such that $a^n b^n \in Q$ but $a^n \notin Q$. Hence there exists m such that $b^{nm} \in \mathbb{Q}$ since Q is primary. Therefore, $b \in \text{rad}(Q)$, and so $\text{rad}(Q)$ is a prime ideal. □

Definition: Let P be a prime ideal. We say that an ideal Q is P-primary if Q is primary and $\text{rad}(Q) = P$. We also say that the prime ideal P is associated with the primary ideal Q.

Theorem VIII.2.10: Let Q and P be ideals. Then, P is prime and Q is P-primary if and only if:

(i) $Q \subsetneqq P \subsetneqq \text{rad}(Q)$,

(ii) If $ab \in Q$ and $a \notin Q$, then $b \in P$.

> **Proof:** Suppose that (i) and (ii) hold. Suppose $ab \in Q$ and $a \notin Q$. Then by (ii), $b \in P$ and so by (i), $b \in \text{rad}(Q)$. So, there exists n such that $b^n \in Q$. Thus, Q is primary.
>
> It remains to show that $\text{rad}(Q) \subsetneq P$. Let $b \in \text{rad}(Q)$ and let n be the smallest number such that $b^n \in Q$. If $n = 1$, then $b \in Q \subseteq P$. If $n > 1$, then $b^{n-1} b \in Q$ and $b^{n-1} \notin Q$, so by (ii), $b \in P$. Hence, $\text{rad}(Q) \subseteq P$. □

Theorem VIII.2.11: If Q_i for $i = 1, \ldots, n$ are P-primary, where P is a prime ideal, then $\bigcap(Q_i)$ is P-primary.

> **Proof:** Let $Q = \bigcap(Q_i)$. Then, $\text{rad}(Q) = \bigcap(\text{rad}(Q_i)) = \bigcap(P) = P$ by a theorem from earlier. Now let $ab \in Q$ and $a \notin Q$. We need to show that $b \in P$. Now, $ab \in Q_i$ for all i, and so $ab \in P$. Thus, $b \in P$. Hence Q is P-primary by the above theorem. □

1.5.3 Section VIII.3 - Primary Decomposition

Let I be an ideal. We say that I has a primary decomposition if we can write $I = Q_1 \cap Q_2 \cap \cdots \cap Q_r$ as the intersection of finitely many primary ideals Q_i.

Definition: If for some i we have $Q_i \supseteq \bigcap_{j \neq i} Q_j$, then $\bigcap_j Q_j = \bigcap_{j \neq i} Q_j$, we say that Q_i is redundant. We'll say that a primary decomposition is irredundant (or reduced) if

(a) No Q_i is redundant.

(b) The $\text{rad}(Q_i)$ are distinct.

We assume that R is a commutative ring with 1 and B is an R-module.

Definition: A proper submodule A of B is primary if

$$r \in R,\ b \notin A,\ rb \in A \implies \exists n, r^n B \subseteq A.$$

This defines primary submodules in a way that makes primary ideals a special case.

Theorem VIII.3.2: Suppose that A is a primary submodule of B. Then, the set $Q_A := \{r \in R \mid rB \subseteq A\}$ is a primary ideal.

> **Proof:** By definition, we have $A \neq B$, and so $1 \notin Q_A$. Thus, $Q_A \neq R$.
>
> Suppose $rs \in Q_A$ with $s \notin Q_A$. Then, $sB \subseteq A$, and so there exists $b \in B$ with $sb \notin A$, but $r(sb) \in A$. Hence there exists n such that $r^n B \subseteq A$, i.e., $r^n \in Q_A$. Thus, Q_A is primary. □

Definition: Let R, B, A, Q_A be as above. Let $P = \text{rad}(Q_A) = \{r \in R \mid \exists n,\ r^n B \subseteq A\}$, a prime ideal. Then we say that A is P-primary.

Definition: Let R, B as above. Let C be a submodule of B. Then, C has a primary decomposition if and only if $C = A_1 \cap \cdots \cap A_n$, where the A_i are primary submodules.

Definition: We say that P_i is an isolated prime if and only if it is minimal with respect to inclusion on the set $\{P_i\}_{i=1}^n$. The others are called embedded primes.

Theorem VIII.3.5: Let R, B, and C be as above. Suppose that

$$C = A_1 \cap \cdots \cap A_k = A'_1 \cap \cdots \cap A'_s$$

are two reduced primary decompositions. Then, $r = s$ and (after reordering) $P_i = P'_i$. If P_i is isolated, then $A_i = A'_i$.

> **Proof:** Consider the set $\{P_1, \ldots, P_k, P'_1, \ldots, P'_s\}$. Assume that P_1 is maximal among these.
>
> We now show that $P_i = P'_j$ for some j. Suppose toward a contradiction that this is not the case. Then, by the maximality of P_1,we have that $P_1 \not\subseteq P'_j$ for all j. By the contrapositive of **Theorem 2.3**, we have that
>
> $$P_1 \not\subseteq (P_2 \cup \cdots \cup P_k \cup P'_1 \cup \cdots \cup P'_s).$$
>
> So, there exists $r \in P_1$ such that $r \notin P_i$ for all $i \geq 2$ and $r \notin P'_j$ for $1 \leq j \leq s$.
>
> Now, A_1 is P_1-primary, so there exists n such that $r^n B \subseteq A$. Using this n, let $C^* = \{x \in B \mid r^n x \in C\}$. If $k = 1$, then $C = A_1$ and so $C^* = B$. We now claim that for $k \geq 1$, $C^* = C$ and that for $k > 1$,

$C^* = A_2 \cap \cdots \cap A_k$. These two facts will then be a contradiction because we assumed that the primary decompositions were reduced.

First, for $k \geq 1$, it's clear that $A_2 \cap \cdots \cap A_k \subseteq C^*$: taking any element on the left and multiplying by r^n, the result is in C, and so the element is in C^*. Additionally, $A_1' \cap \cdots \cap A_s' = C \subseteq C^*$.

Next we show that $C^* \subseteq A_2 \cap \cdots \cap A_k$. Suppose that $x \notin A_i$ for $i \geq 2$. Then, $r^n x \notin A_i$ since if $r^n x \in A_i$, then because A_i is primary, we would have that some power $(r^n)^m = r^{nm}$ would map B into A, which would mean $r^n \in P_i$ since A_i is P_i-primary, and hence $r \in P_i$ since P_i is prime, which is false.

So, $r^n x \notin C$, and thus $x \notin C^*$. Therefore, $C^* \subseteq A_2 \cap \cdots \cap A_k$. Similarly, $C^* \subseteq A_1' \cap \cdots \cap A_s' = C$. Hence $C^* = C$ for $k \geq 1$ and $C^* = A_2 \cap \cdots \cap A_k$ if $k > 1$. If $k = 1$ then we have $B = C$ which is a contradiction. If $k > 1$, then $C = A_2 \cap \cdots \cap A_k$ contradicts the assumption that the decompositions were reduced. Hence, we have proved the claim that, without loss of generality, $P_1 = P_1'$.

We now proceed by induction on k. We first claim that if $k = 1$, then $s = 1$. Suppose $s > 1$. Then, $A_1' \cap \cdots \cap A_s' = A_1$. Consider the corresponding prime ideals $\{P_1', P_2', \ldots, P_s', P_1\}$. if $r \in P_1$ then there exists m with $r^m B \subseteq A_1 = A_1' \cap \cdots \cap A_s' \subseteq A_1'$. So, $r^m B \subseteq A_1'$ and so $r \in P_1$', which means that $r \in P_j'$ for all j. Thus P_1 is not maximal in that set, and we can pick without loss of generality that P_1' is maximal. The previous argument shows that $P_1' = P_1 \subseteq P_2'$. This is a contradiction, and so if $k = 1$ then $s = 1$.

Now assume that $k > 1$ and that the theorem holds for all submodules with a reduced primary decomposition of less than k terms. Let $r \in P_1$. So, there exists n such that $r^n B \subseteq A_1$. Define $C^* := \{x \in B \mid r^n x \in C\}$. It's clear that $A_2 \cap A_3 \cap \cdots \cap A_k \subseteq C^*$. Next we claim that $C^* \subseteq A_2 \cap \cdots \cap A_K$.

Suppose that $x \notin A_j$, with $j \geq 2$. Then, $r^n x \notin A_j$, because if $r^n x \in A_j$ then since A_1 is primary, then there exists m such that $(r^n)^m B \subseteq A_j$ and so $r \in P_j$, which is a contradiction. Since $x \notin A_j$, we have that $r^n x \notin C$ and so $x \notin C^*$. Therefore, $C^* = A_2 \cap \cdots \cap A_k$. Similarly, $C^* = A_2' \cap \cdots \cap A_s'$. Hence

$$C^* = A_2 \cap \cdots \cap A_k = A_2' \cap \cdots \cap A_s'$$

is a reduced primary decomposition of C^*. By the induction hypothesis, we have that $k = s$ and that $P_i = P_i'$ with the correct reordering. This completes the first part of the proof.

It remains to show that if P_i is isolated, then $A_i = A_i'$. Suppose P_i is isolated. Without loss of generality, renumber so that $i = 1$. Since P_1 is isolated, for each $i \neq 1$, there exists $t_i \in P_i \setminus P_1$. Define $t := t_2 \cdots t_k$. Then, $t \in P_i$ for $i \neq 1$ and $t \notin P_1$. Since $t_i \in P_i$, there exists n_i such that $t^{n_i} B \subseteq A_i$. By a similar argument, for each $i \neq 1$, there exists m_i such that $t^{m_i} B \subseteq A_i'$. Let $n := \max\{n_2, \ldots, n_k, m_2, \ldots, m_k\}$. Then, $t^n B \subseteq A_i$ for all $i \geq 2$ and $t^n B \subseteq A_i'$ for all $i \geq 2$.

Let $D = \{x \in B \mid t^n x \in C\}$. We claim that $D = A_1 = A_1'$. If $x \in A_1$, then consider $t^n x$. Since A_1 is a module, $t^n x \in A_1$. But by the above argument, $t^n x \in A_i$ for $i \geq 2$, and so $t^n x \in A_1 \cap \cdots \cap A_k = C$. Thus, $A_1 \subseteq D$.

If $x \in D$, then $t^n x \in C \subset A_1$. However, $t \notin P_1$. Suppose $x \notin A_1$. Then, since $t^n x \in A_1$ and A_1 is primary, there exists some power ℓ such that $(t^n)^\ell B \subseteq A_i$, whence $t \in P_1$, which is a contradiction. Therefore, $x \in A_1$, and so $D \subseteq A_1$. Thus we conclude that $D = A_1$. By an identical argument, $D = A_1'$, and so $A_1 = A_1'$, which completes the proof. $\square$

Theorem VIII.3.6: Suppose R is a commutative ring with 1 and B is an R-module satisfying ACC on submodules. Then, every submodule $A(\neq B)$ has a reduced primary decomposition. In particular, if R is a Noetherian commutative ring with 1, then all finitely generated modules and all proper ideals have reduced primary decompositions.

Proof: Suppose toward a contradiction that there exists an R-module B such that the set $\mathcal{S}$ of proper submodules which do not have a primary decomposition is nonempty. By ACC, the set $\mathcal{S}$ has a maximal element C. In particular, C is not primary. So, there exists $r \in R$ and $b \in B$ such that

$b \notin C$, $rb \in C$, and $r^n B \not\subseteq C$ for all $n \in \mathbb{N}$. Fix r and b. Define $B_m := \{x \in B \mid r^m x \in C\}$. Clearly, $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$, which is an ascending chain of modules. By ACC, there exists k such that $B_k = B_\ell$ for all $\ell \geq k$. It's clear that $B_k \subsetneqq B$. FIx this k.

Let $D := \{x \mid x = r^k y + c, \text{ for some } y \in B \text{ and } c \in C\}$. Now, $C \subseteq B_k \cap D$. We now prove the reverse inclusion. Let $x \in B_k \cap D$. Then we can write $x = r^k y + c$ for some $y \in B$ and $c \in C$. Since $x \in B_k$, we can write $r^k x = r^{2k} y + r^k c$ and so $y \in B_{2k} = B_k$. Thus, $r^k y \in C$, and hence $x \in C$. Therefore, $C = B_k \cap D$.

It remains to prove that B_k and D are proper submodules of B which contain C properly, i.e.,

$$C \subsetneqq B_k \subsetneqq B,$$

$$C \subsetneqq D \subsetneqq B.$$

We have already shown the upper-right inclusion is proper.

Recall that we have $r \in R$ and $b \in B$ with $rb \in C$ and $b \notin C$ such that $r^n B \subsetneqq C$ for all $n \in \mathbb{N}$. Hence, this $b \in B_k \setminus C$, which proves the upper-left inclusion is proper.

If $D \subseteq C$, then $r^k B \subseteq C$, which is a contradiction. This proves that the lower-left inclusion is proper.

Lastly, if $D = B$, then we can write $b = r^k y + c$ with our b above. Then,

$$rb = r^{k+1} y + rc.$$

Well, $rb \in C$ and $rc \in C$, so this implies that $r^{k+1} y \in C$. Thus, $y \in B_{k+1} = B_k$ and so $r^k y \in C$, and so $b \in C$, which is a contradiction. This proves that the lower-right inclusion is proper.

By the maximality of C, we have that B_k and D have primary decompositions. Since $C = B_k \cap D$, we have that C has a primary decomposition, which is a contradiction. $\square$

1.5.4 Section VIII.4 - Noetherian Rings and Modules

We are now equipped to prove some classical theorems.

Theorem VIII.4.1: (I. S. Cohen) Let R be a commutative ring with 1. Then, R is Noetherian if and only if every prime ideal is finitely generated.

> **Proof:** Since every ideal is finitely generated in a Noetherian ring, one direction is obvious. Conversely, suppose that every prime ideal is finitely generated. Let $\mathcal{S} := \{\text{ideals of } R \text{ which are not finitely generated}\}$. Suppose toward a contradiction that $\mathcal{S} \neq \emptyset$. By **Proposition 2.4**, a maximal element of the set $\mathcal{S}$ will be prime, which is a contradiction. Such a maximal element must exist by Zorn's Lemma on the set $\mathcal{S}$. Hence, $S = \emptyset$, so all ideals of R are finitely generated, and thus R is Noetherian. $\square$

Definition: If B is an R-module, then the annihilator of B is the ideal $I := \{r \in R \mid \forall b \in B,\ rb = 0\}$.

Lemma VIII.4.2: Let B be a finitely generated R-module and let I be the annihilator of B in R. Then, B satisfies ACC (resp. DCC) if and only if R/I is a Noetherian (resp. Artinian) ring.

> **Proof:** There is a natural way that B is an R/I module by $(r+I)b = rb$. If R/I is Noetherian, then B is a finitely generated module over a Noetherian ring, and so satisfies ACC. Note that R-submodules of B are the same as R/I-submodules of B. So, ACC on R/I-submodules of B is equivalent to ACC on R-submodules of B. Similarly for DCC.
>
> Conversely, suppose B satisfies ACC. Write $B = Rb_1 + \cdots + Rb_n$ for $b_i \in B$. Let I_j denote the annihilator of Rb_j. Then, $I = \bigcap_{i=1}^{n} I_j$.
>
> We have a monomorphism
>
> $$R/I \longrightarrow R/I_1 \times \cdots \times R/I_n$$
>
> of R-modules. Also, as R-modules
>
> $$R/I_j \cong Rb_j$$
>
> by the mapping $(r+I_j) \mapsto (rb_j + I_j)$. Thus, R/I satisfies ACC, and hence R/I is Noetherian. Similarly for DCC. $\square$

Lemma VIII.4.3: Let P be a prime ideal in a commutative ring with 1. If C is a P-primary submodule of a Noetherian R-module A, then there exists $m \in \mathbb{N}$ such that $P^m A \subseteq C$.

> **Proof:** Let I be the annihilator of A in R and set $\overline{R} := R/I$. For $r \in R$, write $\overline{r}$ for $r + I \in \overline{R}$. Now,
>
> $$P = \{x \in R \mid \exists n\ x^n A \subseteq C\}.$$
>
> So, $I \subseteq P$, and thus $\overline{P} := P/I$ is an ideal of $\overline{R}$. By the **Third Isomorphism Theorem**, $\overline{R}/\overline{P} \cong R/P$, and since R/P is an integral domain, so is $\overline{R}/\overline{P}$. Therefore, $\overline{P}$ is a prime ideal of $\overline{R}$.
>
> Note that $\overline{r}^n A \subseteq C$ if and only if $r^n A \subseteq C$, for all $r \in R$ and $n \in \mathbb{N}$.
>
> Now we check that C is a primary $\overline{R}$-module. Suppose $r + I = \overline{r} \in \overline{R}$ and $a \in A \setminus C$ such that $\overline{r}a \in C$. Then, $ra \in C$ and so there exists n such that $r^n A \subseteq C$, i.e., $\overline{r}^n A \subseteq C$. Thus, C is primary. It is clear that C is in fact $\overline{P}$-primary.
>
> We have that $\overline{R}$ is Noetherian and that C is a $\overline{P}$-primary submodule of A¿ Since $\overline{R}$ is Noetherian, we have that $\overline{P}$ is finitely generated as an ideal. Let $\overline{p_1}, \ldots, \overline{p_s}$ be these generators. By definition of $\overline{P}$-primary, there exists n_i such that $\overline{p_i}^{n_i} A \subseteq C$. If $m = n_1 + \cdots + n_s$, then $\overline{P}^m A \subseteq C$, i.e., $P^m A \subseteq C$. $\square$

Theorem VIII.4.4: (Krull Intersection Theorem) Let R be a commutative ring with 1, I an ideal of R and A a Noetherian R-module. If $B := \bigcap_{n\geq 1} I^n A$, then $IB = B$.

Proof: In the trivial case, $IB = A$. But, we also have $IB \subseteq B \subseteq A$. Hence $B = A = IB$.

Now, assume $IB \neq A$. Consider a (reduced) primary decomposition of IB:

$$IB = A_1 \cap \cdots \cap A_s$$

where A_i is aP_i-primary submodule of A. We want to show $B = A_1 \cap \cdots A_s$. The $\supseteq$ containment is trivial, and so all we need to show is that $B \subseteq A_i$ for all i. Now fix a particular i.

Suppose that $I \subseteq P_i$. Then, by the above **Lemma**, there exists m_i such that $P_i^{m_i} \subseteq A_i$. Now,

$$B = \bigcap (I^n A) \subseteq I^{m_i} A \subseteq P_i^{m_i} A \subseteq A_i$$

and we're done.

Otherwise, suppose that $I \subseteq P_i$. Let $r \in I \setminus P_i$. Suppose that $B \not\subseteq A_i$. Then, there exists $b \in B \setminus A_i$. Now, $rb \in IB \subseteq A_i$. Therefore, there exists m such that $r^m A \subseteq A_i$. Hence, $r \in P_i$, which is a contradiction. $\square$

Lemma VIII.4.5: (Nakayama) Let J be an ideal in a commutative ring with 1. Then, the following are equivalent:

(i) J is contained in every maximal ideal.

(ii) $1 - j$ is a unit for every $j \in J$.

(iii) If A is a finitely generated R-module such that $JA = A$, then $A = 0$.

(iv) If B is a submodule of a finitely generated R-module A such that $JA + B = A$, then $A = B$.

Proof of (i) $\Longrightarrow$ (ii)

Let $j \in J$. If $1 - j$ is not a unit, then there exists a maximal ideal M with $1 - j \in M$. Since $j \in M$, we have that $1 \in M$, which is a contradiction. $\square$

Proof of (ii) $\Longrightarrow$ (iii)

Let A be a finitely generated module such that $JA = A$. Let $a_1, \ldots, a_n$ be a generating set of smallest possible size. Now, $JA = \{j_1 a_1 + \cdots + j_n a_n \mid j_i \in J\}$, and so since $JA = A$, we can write and rearrange:

$$\begin{aligned} a_1 &= j_1 a_1 + j_2 a_2 + \cdots + j_n a_n \\ (1 - j) a_1 &= j_2 a_2 + \cdots + j_n a_n. \end{aligned}$$

Recall that by hypothesis, $1 - j$ is a unit. Hence a_1 is in the R-submodule generated by $a_2, \cdots, a_n$, which contradicts the fact that we picked the generating set of minimal size. Hence, the generating set must have size 0, i.e., $A = 0$. $\square$

Proof of (iii) $\Longrightarrow$ (iv)

Let B be a submodule of a finitely generated R-module A such that $JA + B = A$. Note that A/B is finitely generated, and $J(A/B) = (JA + B)/B = A/B$. Hence by (iii), we have that $A/B = 0$, i.e., $A = B$. $\square$

Proof of (iv) $\Longrightarrow$ (i)

Let M be a maximal ideal. Let $A := R$ and $B := M$. We want to prove that $J \subseteq M$. Suppose toward a contradiction that it's not. Then, $J + M = R$, i.e., $JR + M = R$. By applying (iv), we have that $M = R$, which is a contradiction. Hence J is contained in every maximal ideal. $\square$

Remark: The **Nakayama Lemma** is frequently applied on a local ring (a ring with a unique maximal ideal), with J being the unique maximal ideal.

Proposition VIII.4.6: Let J be an ideal of a commutative ring with identity. Then, J is contained in every maximal ideal if and only if for every Noetherian R-module A, we have $\bigcap_{n\geq 1} J^n A = 0$.

Proof:
($\Longrightarrow$):

Set $B := \bigcap_{n\geq 1} J^n A$. By the **Krull Intersection Theorem**, we have that $JB = B$.

Now, by the **Nakayama Lemma**, we conclude $B = 0$. $\square$

($\Longleftarrow$):

If $R = 0$, the theorem is trivial. So, assume $R \neq 0$. Let M be a maximal ideal of R. Let $A := R/M \neq 0$. Note that R/M is simple and so A is Noetherian. By hypothesis, we have that $\bigcap_{n\geq 1} J^n A = 0$. Since $JA \subseteq A$, we have that either $JA = A$ or $JA = 0$. If $JA = A$, then $J^n A = A$, i.e., $A = \bigcap_{n\geq 1} J^n A = 0$, which is a contradiction. Hence $JA = 0$, i.e., $JR \subseteq M$, i.e., $J \subseteq M$. Since M was arbitrary, J is in every maximal ideal. $\square$

Corollary VIII.4.7: Let R be a Noetherian local ring with maximal ideal M. Then, $\bigcap_{n\geq 1} M^n = 0$.

Proof: Set $J := M$ and $A := R$ in the previous proposition. $\square$

Remark: The above corollary is what is usually called the **Krull Intersection Theorem** by most commutative algebraists. Hungerford rearranges the naming to make it easier to refer to what we call the **Krull Intersection Theorem**.

Remark: Here is an example of the significance of **Corollary 4.7**: Let R be a commutative ring and I an ideal. We can define a topology on R by taking the powers of I as a basis of open neighborhoods of 0, i.e., a subset $U \subseteq R$ is open if and only if for all $x \in U$, there exists n such that $x + U^n \subseteq U$. This is called the I-adic topology.

Example: Let F be a field. Let $R := F[x]$ and let $I := (x)$. Then

$$a \in b + (x^n) \quad \text{if and only if} \quad x^n \mid a - b.$$

We are defining a point to be close to zero if that point is divisible by a high power of x. We can turn this toplogy into a metric space by defining the distance between two points to be small if their difference is divisble by a high power of x. The completion of this topology is $F[[x]]$.

Example: Let $R := \mathbb{Z}$ and $I := (p)$ for a prime p. This gives the p-adic topology. The completion of this topology is $\mathbb{Z}_p$, the p-adic integers.

Proposition VIII.4.8: Let R be a local ring with maximal ideal M. Then every finitely generated projective R-module is free.

Proof: Let P be a finitely generated projective module. Consider

$$F \twoheadrightarrow P$$

with F is free, so that we can pick a basis $\{x_1, \ldots, x_n\}$ for F of minimal size. Then, $\pi(x_1), \ldots, \pi(x_n)$ generate P. Denote $K := \mathrm{Ker}(\pi)$. We now show that $K \subseteq MF$.

If $K \not\subseteq MF$, then there exists $k \in K$ such that $k \notin MF$. Write

$$k = r_1 x_1 + \cdots + r_n x_n$$

and without loss of generality, let $r_1 \notin M$. Now,

$$x_1 - r_1^{-1} k = -r_1^{-1} r_2 x_2 - \cdots - r_1^{-1} r_n x_n.$$

Thus,

$$\pi(x_1) = -r_1^{-1} r_2 \pi(x_2) - \cdots - r_1^{-1} r_n \pi(x_n)$$

So, P is generated by $\pi(x_2), \ldots, \pi(x_n)$, contradicting the minimality of the generating set. So, $K \subseteq MF$. Now, consider the short exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow P \longrightarrow 0$$

we have that $K \oplus P \cong F$ by the isomorphism $(k, 0) \mapsto K$. So, $F = K \oplus P'$, where P' maps isomorphically to P under $\pi\big|_{P'}$. Hence $F \subseteq MF + P'$.

Let $u \in F$. Write $u = \sum(m_i v_i) + p_i$ for $m_i \in M$, $v_i \in F$, and $p_i \in P'$. In F/P', we have that

$$u + P' = \sum(m_i v_i) + P',$$

and so

$$F/P' = M(F/P').$$

By the **Nakayama Lemma**, $F/P' = 0$ and $F = P'$. Therefore, $F \cong P$. $\square$

Theorem VIII.4.9: (Hilbert Basis Theorem) Let R be a commutative Noetherian ring with identity. Then $R[x]$ is Noetherian.

Proof: We show that every ideal of $R[x]$ is finitely generated (as an ideal). Let J be an ideal of $R[x]$. For each $n \geq 0$, let

$$I_n := \{0\} \cup \{r \in R \mid r \text{ is a leading coefficient of a polynomial } f \in J \text{ of degree } n\}.$$

Observe that I_n is an ideal because J is an ideal. If $r \in I_n$, then r is the leading coefficient of some $f \in J$ of degree n. Then, r is also the leading coefficient of $xf \in J$ of degree $n+1$. Hence $r \in I_{n+1}$.

Therefore, we have an ascending chain of ideals in R:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots.$$

By ACC, since R is Noetherian, there exists t such that $I_n = I_t$ for all $t > n$. Also, each I_n is finitely generated.

Suppose $I_n = (r_{n,1}, r_{n,2}, \ldots, r_{n,i_n})$ for $n = 0, 1, \ldots, t$.

For each $r_{n,j}$ with $0 \leq n \leq t$ and $1 \leq j \leq i_n$, choose $f_{n,j} \in J$ of degree n having $r_{n,j}$ as leading coefficient. We claim that

$$J = (X), \quad X := \{f_{n,j} \mid 0 \leq n \leq t, \ \ 1 \leq j \leq i_n\}.$$

Firstly, it's clear that $(X) \subseteq J$. Let $g \in J$ be of degree k. We show by induction on K that $g \in (X)$.

Suppose $k = 0$. Then, $g \in I_0 \subseteq X$, since $f_{0,j} = r_{0,j}$.

Assume $k > 0$ and that all polynomials in J of degree $< k$ lie in (X). Let r be the leading coefficient of g. Note that $r \neq 0$ since $\deg(g) > 0$.

Case 1: $k \leq t$. Then, $r \in I_k$, so we can write $r = s_1 r_{k,1} + \cdots + s_{i_k} r_{k,i_k}$. Then, $s_1 f_{k,1} + \cdots + s_{i_k} f_{k,i_k}$ has leading coefficient r and degree k. Hence,

$$\deg(g - s_1 f_{k,1} + \cdots + s_{i_k} f_{k,i_k})) < k$$

and induction applies.

Case 2: $k > t$. Then, $r \in I_k = I_t$. We can write $r = s_1 r_{t,1} + \cdots + s_{i_t} r_{t,i_t}$, where $r_{t,1}$ are the leading coefficients of polynomials $f_{t,j}$ of degree t in J. Now, $s_1 f_{t,1} + \cdots + s_{i_t} f_{t,i_t}$ has degree t and leading coefficient r. Hence,

$$\deg(g - x^{k-t}(s_1 f_{t,1} + \cdots + s_{i_t} f_{t,i_t})) < k$$

and induction applies. □

Corollary: If R is a commutative Noetherian ring with identity, then $R[x_1, x_2, \ldots, x_n]$ is Noetherian.

Proposition VIII.4.10: Let R be a commutative Noetherian ring with identity. Then $R[[x]]$ is Noetherian.

Proof: We show that every prime ideal is finitely geneated, and then use the theorem of I. S. Cohen which says that if all the prime ideals of a ring are finitely generated, then the ring is Noetherian.

Let P be a prime ideal of $R[[x]]$. Consider the surjective ring homomorphism $R[[x]] \to R$ defined by $\sum a_i x^i \mapsto a_0$. Let P^* be the image of P in R. Then, P^* is an ideal of R, and so is finitely generated. Suppose $P^* = (r_1, \ldots, r_n)$. Let $f_i \in P$ be chosen such that f_i has constant term r_i for $i = 1, \ldots, n$.

Case 1: $x \in P$. In this case, we claim $r_i \in P$ and that $P = (x, r_1, \ldots, r_n)$. Well, since $x \in P$, we can write $f_k = r_k + \sum_{i=1}^{\infty} a_i x^i$ and since $f_k \in P$ and $\sum_{i=1}^{\infty} a_i x^i \in P$, we have that $r_i \in P$. Now, let $g \in P$. Then, $g -$ (constant term of g) $\in (x)$, and the constant term of g is in $(r_1, \ldots, r_n)$. Therefore, $g \in (x, r_1, \ldots, r_n)$, and so $P = (x_1, r_1, \ldots, r_n)$.

Case 2: $x \notin P$. We claim that P is generated by $f_1, \ldots, f_n$. Let $h = \sum_{i=0}^{\infty} c_i x^i \in P$. Write $c_0 = t_1 r_1 + \cdots + t_n r_n$. Now, $h - \sum_{i=1}^{n} t_i f_i = x h^*$ for some $h^* \in R[[x]]$. The left-hand side is in P, and $x \notin P$, so since P is prime, $h^* \in P$. Hence for each $h \in P$, we can find $t_1, \ldots, t_n \in R$ and $h^* \in P$ such that $h = \sum_{i=1}^{n} t_i f_i + x h^*$. (This uses the Axiom of Choice.) Let $\lambda : P \to P$ be defined by $\lambda(h) = h^*$. Let $g \in P$. Then, by the **Recursion Theorem**, there exists $\varphi : \mathbb{N} \to P$ such that $\varphi(0) = g$, $\varphi(k+1) = \lambda(\varphi(k)) = \varphi(k)^*$ for all k. Let $t_{k,i} \in R$ be the coefficients in

$$h_k = \sum_{i=1}^{n} t_{k,i} f_i + x h_{k+1}.$$

Let $g_i := \sum_{k=0}^{\infty} t_{k,i} x^k$ for $0 \leq i \leq n$. Now

$$\begin{aligned} g_1 f_1 + \cdots + g_n f_n &= \sum_{i=1}^{n} \left(\sum_{k=0}^{\infty} (t_{k,i} x^k) \right) f_i \\ &= \sum_{k=0}^{\infty} \left(\sum_{i=1}^{n} (t_{k,i} f_i) \right) x^k \\ &= \sum_{k=0}^{\infty} \left((h_k - x h_{k+1}) \, x^k \right). \end{aligned}$$

So, the sum on the left-hand side of $g_i f_i$ equals the power series on the right-hand side, which is a telescoping sum. There, for each $m \geq 0$, the coefficient of x^m in $g_1 f_1 + \cdots + g_n f_n$ equals the coefficient of x^m on the right-hand side, which equals the coefficient of x^m in $h_0 - x^{m+1} h_{m+1}$, which equals $g - x^{m+1} h_{m+1}$, which equals the coefficient of x^m in g. Hence $g = g_1 f_1 + \cdots + g_n f_n$, which proves our claim of generators. Hence P is finitely generated.

So, all prime ideals are finitely generated, i.e., $R[[x]]$ is Noetherian. $\square$

1.5.5 Section VIII.5 - Ring Extensions

In this section, all rings are commutative.

Definition: If S is a ring with identity and R is a subring containing the identity, then we say that S is a ring extension of R.

Definition: Let S be an extension ring of R and let $s \in S$. If there is a monic polynomial $f(x) \in R[x]$ such that s is a root of $f(x)$, then s is said to be integral over R. If every element of S is integral over R, then we say that S is an integral extension of R.

Remark: Let $R \subset S$ and consider the homomorphism $\text{ev}_s : R[x] \to S$ defined by $\text{ev}_s(r) = r$ for all $r \in R$ and $\text{ev}_s(x) = s$. This is the "evaluation at s" map. Now, s is a root of $f(x)$ if and only if $f(x) \in \text{Ker}(\text{ev}_s)$.

Theorem IX.5.3: Let S be an extension of R and let $s \in S$. Then, the following are equivalent:

(i) s is integral over R.

(ii) $R[s]$ (which is the subring of S generated by R, S) is a finitely generated R-module.

(iii) There exists a subring T of S containing 1 and $R[s]$ which is a finitely generated R-module.

(iv) There exists an $R[s]$-submodule B of S which is finitely generated as an R-module and whose annihilator in $R[s]$ is zero.

Remark: The progression of statements [(i) $\Rightarrow$ (ii)], [(ii) $\Rightarrow$ (iii)], [(iii) $\Rightarrow$ (iv)] appears to be a weakening, and these statements are easy to prove. The real work will be in proving [(iv) $\Rightarrow$ (i)], which shows that this is not really a weakening at all.

Proof: Assume (i). Then, there exists $a_i \in R$ such that

$$s^n + a_{n-1}s^{n-1} + \cdots + a_1 s + a_0 = 0.$$

So for s^k with $k \geq n$ we can write s^k in terms of the s^i with $i < n$. So the module $R[s]$ is generated as an R-module by the set $\{1, s, \ldots, s^{n-1}\}$. Hence (ii) holds.

Assume (ii). If $R[s]$ is a finitely generated R-module, then we can set $T := R[s]$ and since $R[s]$ contains the identity, (iii) holds.

Assume (iii). Let T be as in (iii). Then

$$\text{Ann}_{R[s]}(T) = \{x \in R[s] \mid \forall t \in T,\ xt = 0\}.$$

But, $1 \in T$, and clearly $x1 = 0$ implies $x = 0$. Therefore $\text{Ann}_{R[s]}(T) = \{0\}$. Hence (iv) holds.

Assume (iv). Let B be generated over R by $b_1, \ldots, b_n$. Since B is an $R[s]$-module, we have $sb_i \in B$ for all $i = 1, 2, \ldots, n$. So, we can write

$$\begin{aligned} sb_1 &= r_{1,1}b_1 + r_{1,2}b_2 + \cdots + r_{1,n}b_n \\ sb_2 &= r_{2,1}b_1 + r_{2,2}b_2 + \cdots + r_{2,n}b_n \\ &\vdots \qquad\qquad\qquad\qquad \vdots \\ sb_n &= r_{n,1}b_1 + r_{n,2}b_2 + \cdots + r_{n,n}b_n \end{aligned}$$

Let M denote the matrix $(r_{i,j})_{i,j=1}^n$. Then, $M - sI_n$ is an $n \times n$ matrix with coefficients in $R[s]$. The equations can be written

$$(M - sI_n)\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \qquad (\dagger)$$

Remark: Let A be an $n \times n$ matrix. Let A_{ij} denote the matrix you get when you remove the i^{th} row and the j^{th} column. Set A^* to be the matrix whose i,j entry is $(-1)^{i+j}A_{ji}$. Then, we have the formula $A^* \cdot A = (\det(A))I_n$. This is from other algebra courses, and is sometimes called Cramer's Rule. From this, we have that if $A \cdot b = c$, then $A^*A \cdot v = A^* \cdot c$ and hence $(\det(A))I_n \cdot b = A^* \cdot c$.

So, from (†), we have that if $d := \det(M - sI_n) \in R[s]$, then we have

$$d \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

i.e., $db_i = 0$ for all $i = 1, 2, \ldots, n$. Hence $d \in \text{Ann}_{R[s]}(B) = \{0\}$, i.e., $d = 0$. But $\pm d$ is a monic polynomial of degree n in s with coefficients in R. Hence, s is integral over R. □

Corollary: If S is a ring extension of R and S is finitely generated as an R-modoule, then S is an integral extension of R.

Theorem: If S is an extension of R and $s_1, \ldots, s_n \in S$ are integral over R, then $R[s_1, \ldots, s_n]$ is a finitely generated R-module and an integral extension of R.

Proof: (Sketch) Consider

$$R \subset R[s_1] \subset R[s_1, s_2] \subset \cdots \subset R[s_1, \ldots, s_n].$$

And note that each extension is integral and we can set up appropriate generators.

Theorem IX.5.6: If T is an integral extension of S and S is an integral extension of R, then T is an integral extension of R.

Remark: Recall that if R is Noetherian, then $R[x]$ is Noetherian. Hence $R[x_1, \ldots, x_n]$ is Noetherian. (This is the Hilbert Basis Theorem.) So if A is an R-algebra which is finitely generated as an R-algebra, then $A \cong R[x_1, \ldots, x_n]/I$ for some ideal I, and hence A is Noetherian. In particular, if A is finitely generated as an R-module, then A is Noetherian.

So, if B is a subring of A, and A is finitely generated as a module over B, and if B is Noetherian, then A is Noetherian. The converse of this theorem is true and is called the **Eakin-Nagata Theorem**. The proof of this converse is not in the book, but there is an easy version of it due to E. Formanek.

Integral Extensions

Theorem: Let S be an extension ring of R and let $\widehat{R}$ be the set of all elements of S that are integral over R. Then, $\widehat{R}$ is a ring containing every subring of S which is integral over R.

Proof: Let $s, t \in \widehat{R}$. Then, $s, t \in R[s,t]$ and so $s - t \in R[s,t]$ and $st \in R[s,t]$. Since s, t are integral over R, we have that $R[s,t]$ is an integral extension of R. Therefore, $s - t$ and st are integral over R. This shows that $\widehat{R}$ is a ring. □

Definition: $\widehat{R}$ is called the integral closure of R in S. We say that an integral domain R is integrally closed if R equals the integral closure of R in its field of fractions.

Example: $\mathbb{Z}$ is integrally closed (in the rational field $\mathbb{Q}$).

Example: $\mathbb{Z}$ is not integrally closed in $\mathbb{C}$, because i satisfies $x^2 + 1 \in \mathbb{Z}[x]$, so i is integral over $\mathbb{Z}$.

Exercise: Every Unique Factorization Domain is integrally closed.

Theorem: Let T be a multiplicative subset of an integral domain R such that $0 \notin T$. If R is integrally closed, then $T^{-1}R$ is integrally closed.

Remark: Letting $Q(X)$ denote the field of fractions of an arbitrary ring X, we can think of the ring $T^{-1}R$ as lying between R and $Q(R)$, i.e.,

$$R \subset T^{-1}R \subset Q(R).$$

Additionally, it's clear that $Q(T^{-1}R) = Q(R)$.

Proof: Let $u \in Q(R)$ be integral over $T^{-1}R$. Then, we can write

$$u^n + \left(\frac{r_{n-1}}{s_{n-1}}\right) u^{n-1} + \cdots + \left(\frac{r_1}{s_1}\right) u + \left(\frac{r_0}{s_0}\right) = 0$$

for $r_i \in R$ and $s_i \in T$. Let $s := s_0 \cdots s_{n-1}$, and multiply the above equation by s^n to get

$$(su)^n + r'_{n-1}(su)^{n-1} + \cdots + r'_1(su) + r'_0 = 0$$

where $r'_i \in R$. So, su is integral over R and hence $su \in R$ because R is integrally closed. Thus, $u \in T^{-1}R$, since $s \in T$. $\square$

Theorem: (Lying-Over Theorem) Let S be an integral extension of R and let P be a prime ideal of R. Then, there exists a prime ideal Q of S such that $Q \cap R = P$.

Proof: Since P is prime, $R \setminus P$ is a multiplicative set of R, and hence also of S. By a standard lemma (**Theorem 2.2**), there exists a prime ideal Q of S which is maximal among all ideals I of S such that $I \cap (R \setminus P) = \emptyset$.

Then, $Q \cap R$ is a prime ideal of R and $Q \cap R \subseteq P$. It remains to prove that $Q \cap R = P$.

Suppose not. Then there exists $u \in P \setminus (Q \cap R)$. Then, $u \notin Q$ and so $Q + (u) \supsetneq Q$, hence by the maximality of Q, we have that $(Q + (u)) \cap (R \setminus P) \neq \emptyset$. Let $c \in (Q + (u)) \cap (R \setminus P)$. Write c as $q + su$ for $q \in Q$ and $s \in S$. Since s is integral over R we can write

$$s^n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0.$$

Multiply by u^n to get

$$(us)^n + (r_{n-1}u)(us)^{n-1} + \cdots + r_1 u^{n-1}(us) + r_0 u^n = 0.$$

Now $us = c - q$, hence by the binomial theorem, we have that

$$v = c^n + (r_{n-1}u)c^{n-1} + \cdots + r_1 u^{n-1}c + r_0 u^n \in \mathbb{Q}.$$

Since $v \in R$, so $v \in R \cap Q \subset P$, but $u \in P$ hence $c^n \in P$. This is a contradiction, since $c \in R \setminus P$. Thus, $Q \cap R = P$. $\square$

Corollary VIII.5.10: (Going-Up Theorem) Let S be an integral extension of R and let $P_1 \subset P$ be prime ideals of R. If Q_1 is a prime ideal of S lying over P_1, then there exists a prime ideal Q of S such that $Q_1 \subset Q$ and Q lies over P.

Proof: $R \setminus P$ is a multiplicative set of S, and since $Q_1 \cap R = P_1 \subset P$, we have that $Q_1 \cap (R \setminus P) = \emptyset$. So, Q_1 is an ideal of S distinct from $R \setminus P$. So, there exists a prime ideal of $S \subset Q$ which is maximal in the set of ideals containing Q_1 and dijoint from $R \setminus P$.

Clearly, $Q \cap R \subseteq P$, so it remians to show that $Q \cap R = P$. Suppose $u \in P \setminus (Q \cap R)$. Then, $Q + (u)$ properly contains Q and so by the maximality it intersects $R \setminus P$. Let $c = q + su$ be an element of the intersection. Since S is integral over R, we have that

$$s_n + r_{n-1}s^{n-1} + \cdots + r_1 s + r_0 = 0 \in Q.$$

Now,

$$(su)^n + r_{n-1}u(su)^{n-1} + \cdots + nu^{n-1}(su) + r_0 u^n = 0 \in Q,$$

i.e.,

$$c^n + r_{n-1}uc^{n-1} + \cdots + r_1 u^{n-1}c + r_0 u^n \in Q.$$

Therefore, $c^n \notin Q$ and so $c \in Q \cap R \subset P$, which is a contradiction. $\square$

Theorem VIII.5.11: Let S be integral over R and P be a prime ideal of R. If Q and Q' are prime ideals of S lying over P, and $Q \subset Q'$, then $Q = Q'$.

Proof: We show that if Q is a prime ideal of S and $Q \cap R = O$, then Q is maximal in the set of ideals I in S such that $I \cap (R \setminus P) = \emptyset$.

Suppose Q is not maximal in S. Then, there exists I such that $Q \subsetneq I$, Then, $I \cap R \subseteq P$. Choose $u \in I \setminus Q$. Then, u is integral over R¡ and hence

$$\{f(x) \in R[x] \mid f(u) \in Q,\ f \text{ monic}, \deg(f) = 1\} \neq \emptyset.$$

Pick an element $f(x)$ from this set of smallest degree. Write $f(x)$ as

$$f(x) = \sum r_i x^i.$$

Then,

$$u^n + r_{n-1}u^{n-1} + \cdots + r_1 u_1 + r_0 \in Q \subset I.$$

Hence, $r_- \in I \cap R \subset P \subset Q$, and now

$$u(\underbrace{u^{n-1} + r_{n-1}u^{n-2} + \cdots + r_1}_{\notin Q, \text{ by minimality of } \deg(f)}) \in Q.$$

Hence, $u \in Q$, which is a contradiction $\square$

Theorem VIII.5.12: Let S be an integral extension of R. Let Q be a prime ideal of S lying over a prime ideal P of R. Then, Q is maximal in S if and only if P is maximal in R.

Proof: Suppose Q is maximal and P_1 is a maximal ideal of R containing P. Then, by the **Going-Up Theorem**, there exists Q_1 containing Q such that $Q_1 \cap R = P_1$. But, Q is maximal, and so $Q = Q_1$ and $P = P_1$, i.e., P is maximal.

Now suppose P is maximal. Let Q_1 be a maximal ideal of S containing Q. Then, $Q_1 \cap R$ is a prime ideal of R containing P. By the maximality of P, we have that $Q_1 \cap R = P$. Thus, $Q \subset Q_1$ and Q and Q_1 both lie over P, hence $Q = Q_1$, i.e., Q is maximal. $\square$

1.5.6 Section VIII.6 - Dedekind Domains

Definition: A Dedekind Domain is an integral domain with every proper ideal a product of prime ideals.

Definition: Let R be an integral domain with field of fractions K. An R-submodule I of K is called a fractional ideal if there exists $a \in R$ such that $aI \subseteq R$.

Example: With the hypotheses above, any finitely generated submodule of K is a fractional ideal.

Remark: If I is a fractional ideal such that $aI \subseteq R$, then aI is an ideal of R and $I \cong aI$ as R-modules.

Remark: If I, J are fractional ideals, then we define

$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N},\ a_i \in I,\ b_i \in J \right\}.$$

Definition: We say that a fractional ideal I is invertible if there exists a fractional ideal J such that $IJ = R$.

Remark: The fractional ideals form a monoid and the invertible fractional ideals form a group.

Notation: If I is any fractional ideal, then we define

$$I^{-1} := \{a \in K \mid aI \subseteq R\}.$$

Remark: If I is invertible, then I^{-1} is the inverse of I in the group of invertible fractional ideals. If J is the inverse of I, then $JI = R$ so $J \subseteq I^{-1}$. Conversely since I^{-1} and J are R-submodules of K, we have that

$$I^{-1} = RI^{-1} = (JI)I^{-1} = J(II^{-1}) \subset JR = RJ \subset J.$$

Hence $J = I^{-1}$ and so the inverse of I is actually I^{-1} when it exists.

Remark: Every principal ideal is invertible, because $(a) = (a^{-1})$.

Lemma VIII.6.4: Let $I, I_1, \ldots, I_n$ be ideals of an integral domain R. Then,

(i) $I_1 I_2 \cdots I_n$ is invertible if and only if each I_j is invertible.

(ii) If $P_1 \cdots P_m = I = Q_1 \cdots Q_n$ where P_i and Q_j are prime and each P_i is invertible, then $m = n$ and after renumbering we have $P_i = Q_i$.

Proof of (i): Suppose $I_1 I_2 \cdots I_n$ is invertible. Then, there exists J such that

$$R = (I_1 I_2 \cdots I_n)J = I_1(I_2 \cdots I_n J).$$

Hence I_1 is invertible, and continue the process for each I_j.

Conversely if each I_j is invertible then for each j was have $I_j I_j^{-1} = R$, and so

$$(I_1 \cdots I_n)(I_1^{-1} \cdots I_n^{-1}) = R.$$

Thus, $I_1 I_2 \cdots I_n$ is invertible. $\square$

Proof of (ii): (By induction on m) In the case $m = 1$, we have that $P_1 = I = Q_1 \cdots Q_n$, and so $P_1 \subseteq Q_j$ for all j. Since P_1 is prime, there exists h such that $Q_j \subseteq P_1$. Hence $P_1 = Q_1$, and thus $P_1 = P_1 Q_2 \cdots Q_n$. Since P_1 is invertible, we have that $Q_2 \cdots Q_n = R$, which is a contradiction. So, $n = 1$.

Now suppose $m > 1$. Choose P_1 to be minimal among the P_i. Then,

$$Q_1 \cdots Q_n = P_1 \cdots P_m \subset P_1.$$

Since P_1 is prime, there exists j with $Q_j \subset P_1$. (To see this, consider $AB \subseteq P$ with $B \not\subseteq P$. Pick $b \in B$ with $b \notin P$. Then for all $a \in A$, we have that $ab \in AB \subseteq P$ but $b \notin P$ and so $a \in P$. Hence $A \subseteq P$.) Say without loss of generality that $Q_1 \subseteq P_1$. We similarly have that

$$P_1 \cdots P_m = Q_1 \cdots Q_n \subset Q_1.$$

So there exists P_j such that $P_j \subseteq Q_1 \subseteq P_1$, but by the minimality of P_1 we must have that $j = 1$ and $Q_1 = P_1$. Since $P_1 = Q_1$ is invertible, we can cancel them (see **Remark (ii), pg. 402**) to get that

$$Q_2 \cdots Q_n = P_2 \cdots P_m$$

and apply the induction hypothesis to get $m = n$ and after reordering $P_i = Q_i$ for all i. □

Theorem VIII.6.5: If R is a Dedekind Domain, then every nonzero prime ideal is invertible and maximal.

Proof: First we show that invertible prime ideals are maximal. Let P be an invertible prime ideal. We show that for $a \in R \setminus P$ we have that $P + Ra = R$. Suppose not. Then, $P + Ra$ is proper and so

$$P + Ra = P_1 \cdots P_m$$

for P_i prime ideals. Also

$$P + Ra^2 \subseteq P + Ra \subsetneq R$$

is proper, and hence we can write

$$P + Ra^2 = Q_1 \cdots Q_n$$

for Q_i prime ideals. We will now work in the integral domain R/P. Let bar notation denote passage from R to R/P by the canonical reduction map.

We now have that

$$\begin{aligned}(\overline{a}) &= \overline{P_1} \cdots \overline{P_m},\\ (\overline{a})^2 = (\overline{a}^2) &= \overline{Q_1} \cdots \overline{Q_n}.\end{aligned}$$

Since principal ideals are invertible we have that both $(\overline{a})$ and $(\overline{a}^2)$ are invertible, and therefore by **Lemma VIII.6.5** so are the $\overline{P_i}$ and $\overline{Q_i}$.

Now note that $(\overline{a})^2 = \overline{P_1}^2 \cdots \overline{P_m}^2$, and hence $n = 2m$ and after renumbering, $\overline{P_i} = \overline{Q_{2i-1}} = \overline{Q_{2i}}$ for $i = 1, \ldots, m$ (i.e., $\overline{P_1} \cdots \overline{P_n} = \overline{Q_1 Q_1} \cdots \overline{Q_m Q_m}$). We can remove the bars to conclude similarly that $P_i = Q_{2i-1} = Q_{2i}$. Therefore

$$P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra.$$

So, if we choose $b \in P$, we can write $b = c + ra$ with $c \in P^2$ and $r \in R$. Then, $ra \in P$ and therefore $r \in P$ since $a \notin P$ and P is prime. Now, we have the inclusions (added to the right of the above inclusions)

$$P \subseteq P + Ra^2 = (P + Ra)^2 \subseteq P^2 + Ra \subseteq P^2 + Pa \subseteq P$$

and so we have equality throughout. So $P = P^2 + Pa = P(P + Ra)$. Therefore, $R = P + Ra$ which is a contradiction since we assumed that $P + Ra$ was proper. So, we have shown that every invertible prime ideal is maximal.

Now let P be any prime ideal and let $c \in P$ be nonzero. Then, $P \supseteq (c) = P_1 \cdots P_m$ where the P_i are prime, (c) is invertible. Thus the P_i are invertible. Therefore, $P_k \subseteq P$ for some k. By the maximality of P_k we have $P_k = P$ and hence P is maximal and invertible. $\square$

Lemma VIII.6.7: Every invertible fractional ideal of an integral domain R (with fractional field K) is finitely generated.

Proof: Let I be an invertibel fractional ideal. Recall that $I^{-1} := \{a \in K \mid aI \subseteq R\}$ and invertibility means $I^{-1}I = R$. In other words, there exists $a_i \in I^{-1}$ and $b_i \in I$ such that $\sum a_i b_i = 1$ for $i = 1, 2, \ldots, n$.

Let $c \in I$. Then

$$c = c1 = c\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} \underbrace{(ca_i)}_{\in R} b_i.$$

So, any element of I can be written as an R-linear combination of the b_i, i.e., $b_1, \ldots, b_n$ generate I. $\square$

Corollary: Dedekind Domains are Noetherian.

Lemma VIII.6.6: If I is a fractional ideal of an integral domain R with fractional field K and $f \in \mathrm{Hom}_R(I, R)$, then for all $a, b \in I$ we have that $af(b) = bf(a)$.

Proof: Let $a = r/s$ and $b = v/t$ for $r, s, v, t \in R$. Now, $sab = rb \in I$ and $tab = va \in I$. Observe that

$$\begin{aligned} sf(tab) &= f(stab) \\ &= tf(sab). \end{aligned}$$

We now compute that

$$af(b) = \frac{sa}{s} f(b) = \frac{1}{s} f(sab) = \frac{1}{t} f(tab) = \frac{tb}{t} f(a) = bf(a). \ \square$$

Theorem VIII.6.8: Let R be an integral domain and I a fractional ideal. Then I is invertible if and only if I is a projective R-module.

Proof:
($\Longrightarrow$):

Suppose I is invertible. Then I is finitely generated by some $b_1, b_2, \ldots, b_n$. Since I is invertible, we can find a_i such that $1 = \sum a_i b_i$. Consider the free module with basis $e_1, \ldots, e_n$

$$\begin{aligned} \bigoplus R_{e_i} &\xrightarrow{\varphi} P \\ e_i &\longmapsto b_i \end{aligned}$$

We'll show that φ splits; then, $I \cong$ the direct summand of a free module, hence I is projective. Define

$$\begin{aligned} I &\xrightarrow{\xi} \bigoplus R_{e_i} \\ c &\longmapsto c\sum a_i e_i \end{aligned}$$

Observe that ξ is an R-module homomorphism. Now,

$$\begin{aligned} \varphi \circ \xi(c) &= \varphi(c\sum a_i e_i) \\ &= c\sum a_i b_i \\ &= c. \end{aligned}$$

Hence $\varphi \circ \xi = \mathrm{Id}$. Thus φ splits. $\square$

($\Longleftarrow$):

Conversely, assume that I is projective. Let $X := \{b_j \mid j \in j\}$ be a set of generators of I. Fix an element $b_0 \in X$. Since I is projective, the function φ in the diagram below splits, i.e., there exists $\psi : I \to \oplus R_{e_i}$ such that $\varphi \circ \psi = \mathrm{Id}$:

$$\begin{array}{ccc} \bigoplus R_{e_i} & \underset{[e_i \mapsto b_i]}{\overset{\varphi}{\rightleftarrows}} & I \\ \downarrow \pi_j & & \\ R_{e_j} \cong R & & \end{array}$$

Let $\theta_j := \pi_j \circ \psi : I \to R_{e_j} \cong R$, mapping $re_j \mapsto r$. Let $c_j \in R$ be defined as $\theta_j(b_0)$. Note that $\theta_j \in \mathrm{Hom}_R(I, R)$. Let $c \in I$. Then,

$$cc_j = c\theta_j(b_0) = b_0\theta_j(c).$$

Hence

$$c(c_j/b_0) = \frac{b_0\theta_j(c)}{b_0} = \theta_j(c) \in R.$$

Therefore, $\dfrac{c_j}{b_0} \in I$ for all j.

For any $c \in I$, we can write for $|J_1|$ finite:

$$\psi(c) = \sum_{j \in J_1} \theta_j(c) e_j.$$

Now,

$$\begin{aligned} c &= \varphi\psi(c) \\ &= \varphi\left(\sum_{j \in J_1} \theta_j(c) e_j\right) \\ &= \sum_{j \in J_1} c\frac{c_j}{b_0} b_j \\ &= c\left(\sum_{j \in J_1} \frac{c_j b_j}{n_0}\right). \end{aligned}$$

Hence

$$\sum_{j \in J_1} \underbrace{\frac{c_j}{b_0}}_{\in I^{-1}} \underbrace{b_j}_{\in I} = 1$$

and so I is invertible. $\square$

Definition: A discrete valuation ring (or, DVR) is a principal ideal domain which has exactly one nonzero prime ideal.

Example: The ring $\mathbb{Z}_{(p)} := \left\{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\right\}$ is a discrete valuation ring.

Example: The ring $K[x]_{(x)} = \left\{ \frac{f(x)}{g(x)} \in K(x) \mid x \nmid g(x) \right\}$ is a discrete valuation ring.

Lemma VIII.6.9: If R is a Noetherian integrally closed integral domain with a unique nonzero prime ideal P, then R is a discrete valuation ring.

Proof: We want to show that every ideal is principal.

(i) Let $K = \text{frac}(R)$. For every fractional ideal I, the set $\overline{I} = \{a \in K \mid aI \subseteq I\}$ is equal to R.

Note that $\overline{I}$ is a subalgebra of K containing R. To see that $\overline{I} = R$, observe that $\overline{I}$ is also a fractional ideal and is an R-subgroup of K. Additionally, $\overline{I}$ is finitely generated and so it is an integral extension of R, which is integrally closed, so $\overline{I} = R$. To see that $\overline{I}$ is finitely generated, let J be any fractional ideal. Then there exists $b \in R$ such that $bJ \subseteq R$. Clearly the map $J \to bJ$ defined by $x \mapsto bx$ is an R-module isomorphism. Since R is Noetherian, bJ is finitely generated (as it is an ideal of R) and hence so is J.

(ii) $R \subsetneqq P^{-1}$.

Let S be the set of ideals of R such that $R \subsetneqq I^{-1}$. Let $a \in P$ be nonzero. Then $1/a \notin R$, but $1/a \in (a)^{-1}$. So, $(a) \in S$, i.e., $S \neq \emptyset$. Since R is Noetherian, we can use the maximality condition to find a maximal element M of S. We now show that M is prime, i.e., $M = P$. Suppose $a, b \in R$ with $ab \in M$ and $a \notin M$. Let $c \in M^{-1} \setminus R$. Then, $bc(aR + M) \subseteq R$. Therefore, $bc \in (aR + M)^{-1}$. By the maximality of M, we have that $aR + M \notin S$ and hence $bc \in R$. Therefore, $c(bR + M) \subseteq R$ and so $c \in (br + M)^{-1}$ but $c \notin R$ by assumption. Therefore $bR + M \in S$. By maximality of M this implies $b \in M$ which proves that M is a prime idea and so $M = P$. Therefore $P \in S$ which proves this fact.

(iii) P is invertible.

If $PP^{-1} \subsetneqq R$, then $PP^{-1} \subseteq P$ (since it's an ideal so can't be bigger than P since P is unique prime) and so $P^{-1} \subseteq \overline{P}$. Then,

$$\underbrace{R \subsetneqq P^{-1}}_{\text{by (ii)}} \subseteq \underbrace{\overline{P} = R}_{\text{by (i)}}$$

which is a contradiction. So, $PP^{-1} = R$ and P is invertible.

(iv) $\bigcap_{n \geq 1} P^n = \{0\}$.

Suppose $\cap P^n \neq 0$. Then $\cap P^n$ is a fractional ideal. Also, $P^{-1} \subseteq \overline{\cap P^n}$. Then,

$$\underbrace{R \subsetneqq P^{-1}}_{\text{by (ii)}} \subseteq \underbrace{\overline{\cap P^n} = R}_{\text{by (i)}}$$

which is a contradiction. So, $\cap P^n = 0$

(v) P is principal.

Since $\cap P^n = \{0\}$ there exists$a \in P \setminus P^2$. Then, aP^{-1} is a nonzero ideal of R and $aP^{-1} \not\subseteq P$ since otherwise

$$a \in aRaP^{-1}P \subseteq P^2.$$

So $aP^{-1} = R$. Thus $(a) = P$.

Now we use these five facts. Let I be a nonzero proper ideal. Then, $I \subseteq P$. By (iv), there exists m such that $I \subseteq P^m$ but $I \not\subseteq P^{m+1}$. Suppose by (v) that $P = (a)$. Let $b \in I \setminus P^{m+1}$. Then, $b = a^m u$ for some $u \in R$, since $P^m = (a^m)$. We now claim that u is a unit. If not, then $(u) \subsetneq P$ and so $a \mid u$. Hence, $a^{m+1} \mid b$ which is a contradiction since $b \notin P^{m+1}$. So, $P^m = (a^m) = (b) \subseteq I$. Thus, $I = P^m = (a^m)$. $\square$

Proposition: Let R be an integral domain and view R_P (P prime) as a subring of $\text{frac}(R) =: K$. Let $\mathscr{M}$ be the set of all maximal ideals of R. Then, $\bigcap_{M \in \mathscr{M}} R_M = R$.

Proof: Let $u \in K$ and set $D(u) = \{a \in R \mid au \in R\}$. Note that)$D(u$ is an ideal of R, and $D(u) = R$ if and only if $1 \in D$ if and only if $u \in R$.

Let M be a maximal ideal. An element $v \in K$ belongs to R_M if and only if there exists $t \in R \setminus M$ such that $tu \in R$ if and only if $D(v) \cap (R \setminus M) \neq \emptyset$ if and only if $D(v) \not\subseteq M$.

Thus, $v \in \bigcap_{M \in \mathscr{M}} R_M$ if and only if $D(v) \not\subseteq M$ for any maximal ideal M if and only if $D(v) = R$ if and only if $v \in R$. $\square$

Theorem VIII.6.10: If R is an integral domain, then the following are equivalent.

(i) R is a Dedekind Domain.

(ii) Every proper ideal in R is uniquely a product of a finite number of prime ideals.

(iii) Every nonzero ideal in R is invertible.

(iv) Every fractional ideal of R is invertible.

(v) The set of all fractional ideals of R is a group under multiplication.

(vi) Every ideal in R is projective.

(vii) Every fractional ideal of R is projective.

(viii) R is Noetherian, integrally closed, and every nonzero prime ideal is maximal.

(ix) R is Noetherian and for every nonzero prime ideal P of R, the localization of R_P of R at P is a discrete valuation ring.

Proof: We have already proved the following equivalences: (iv) $\Leftrightarrow$ (v) (Theorem VIII.6.3), (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) (Lemma VIII.6.4 and Theorem VIII.6.5), (iii) $\Leftrightarrow$ (vi) and (vii) $\Leftrightarrow$ (iv) (Theorem VIII.6.8), (vi) $\Rightarrow$ (vii) (remark regarding isomorphism prior to Theorem VIII.6.3).

It remains to prove (iv) $\Rightarrow$ (viii), (viii) $\Rightarrow$ (ix), (ix) $\Rightarrow$ (i).

(iv) $\Longrightarrow$ (viii):

Assume R is an integral domain and every fractional ideal is invertible. So, for every ideal I, we can find an ideal I^{-1} such that $II^{-1} = R$, i.e., $\sum a_i b_i = 1$ for $a_i \in I^{-1}$, $b_i \in R$. So, there exists $c \in R$ such that $\sum (ca_i)b_i \in (b_1, b_2, \ldots, b_n)$. This shows that R is finitely generated, and hence Noetherian. (See **Lemma VIII.6.7**).

Now let $K := \text{frac}(R)$. Let $u \in K$ be integral over R. Then, $R[u]$ is finitely generated as an R-module by integrality of u, hence is a fractional ideal, and so is invertible by assumption. Observe that $R[u]R[u] = R[u]$. Therefore,

$$R[u] = RR[u] = \underbrace{(R[u]^{-1}R[u])}_{R} R[u] = R[u]^{-1}(R[u]R[u]) = R[u]^{-1}R[u] = R.$$

Hence R is integrally closed.

Let P be a nonzero prime ideal. Then, there exists a maximal ideal M with $P \subseteq M$. Now, M is invertible and $M^{-1}P$ is a fractional ideal. Note that $M^{-1}P \subseteq M^{-1}M = R$, and so $M^{-1}P$ is an ideal. Then, $M(M^{-1}P) = P$. Since P is prime, we have $M \subseteq P$ or $M^{-1}P \subseteq P$. Now, if $M \subseteq P$, then $P = M$ is maximal. Otherwise, $M^{-1}P \subseteq P$, and then $R \subseteq M^{-1} = M^{-1}R = (M^{-1}P)P^{-1} \subseteq PP^{-1} = R$, and so we have equality throughout. Thus, $R = M^{-1}$ and so $R = MM^{-1} = MR = M$, which is a contradiction. Therefore, we have that P is maximal. $\square$

(viii) $\Longrightarrow$ (ix):

If R is integrally closed, then R_P is integrally closed by **Theorem VIII.5.8**. The ideals of R_P are of the form $I_P = \{i/s \mid i \in I, s \in R \setminus P\}$, where I is an ideal of R. (Note that if $I \not\subseteq P$, then $I_P = R_P$.) Since R is Noetherian, every ideal I of R is finitely genenerated. Hence every ideal I_P of R_P is finitely generated and so R_P is Noetherian.

By **Theorem III.4.11**, every prime ideal of R_P is of the form I_P where I is a prime ideal of R contained in P. By the assumption that every nonzero prime ideal is maximal, so the set of nonzero prime ideals of R containing P consists only of P. Hence P_P is the unique nonzero prime ideal of R_P. Now, by **Lemma VIII.6.9**, R_P is a discrete valuation ring. $\square$

(ix) $\Longrightarrow$ (i):

First we show that every nonzero ideal is invertible. Let I be a nonzero ideal of R. Then, $I^{-1} = \{a \in K \mid aI \subseteq R\}$. We know that $II^{-1} \subseteq R$ and II^{-1} is a fractional ideal, and so II^{-1} is an ideal of R.

Suppose toward a contradiction that $II^{-1} \neq R$. Then, there exists a maximal ideal M such that $II^{-1} \subseteq M$. Now we consider localizations. Let $I_M \subseteq R_M$. Note that I_M is principal by the hypothesis of (ix). So, $I_M = \left(\frac{a}{s}\right)$ for some $a \in I$ and $s \in R \setminus M$. R is Noetherian, so $I = (b_1, \ldots, b_m)$ is finitely generated.

Note that $\frac{b_i}{1} \in I_M$ and so for each i,

$$\frac{b_i}{1} = \frac{r_i}{s_i} \cdot \frac{a}{s}$$

for some $r_i \in R$ and $s_i \in R \setminus M$.

So, $ss_ib_i = r_ia \in I$. Let $t = ss_1 \cdots s_m$. Then, for all i

$$tb_i = ss_1 \cdots s_m b_i = s_1 \cdots s_{i-1}s_{i+1} \cdots s_m r_i a_i.$$

So for all i,

$$\frac{t}{a}b_i = s_1 \cdots s_{i-1}s_{i+1} \cdots s_m r_i \in R.$$

Hence $\frac{t}{a} \in I^{-1}$ and so $t = \frac{t}{a}a \in I^{-1}I \subseteq M$, which is a contradiction. Therefore, we have shown that every nonzero ideal is invertible.

Now we discuss a construction we will use shortly. For any proper ideal I, let M_I be a maximal ideal containing I. Then,

$$IM_I^{-1} \subseteq M_I M_I^{-1} = R,$$

and so IM_I^{-1} is an ideal of R. We claim that $I \subsetneqq IM_I^{-1}$. Assume toward a contradiction that $I = IM_I^{-1}$. Then, $R = M_I^{-1}$ and so $R = M_I$, which a contradiction. So, indeed $I \subsetneqq IM_I^{-1}$.

Let J be an arbitrary nonzero proper ideal of R. Set $J_0 = J$, $J_1 = J_0 M_{J_0}^{-1}$, $J_2 = J_1 M_{J_1}^{-1}$, etc. Now,

$$J = J_0 \subsetneqq J_1 \subsetneqq J_2 \subsetneqq J_3 \subsetneqq \cdots \subsetneqq J_{k-1} \subsetneqq J_k = J_{k+1}$$

where this theorem stabilizes since R is Noetherian. Pick k so that it is minimal. Now, $J_{k-1}M_{J_{k-1}}^{-1} = R$, and so $J_{k-1} = M_{J_{k-1}}$. Hence, $J_{k-2}M_{J_{k-1}}^{-1} = J_{k-1} = R$, and so $J_{k-2} =$

$M_{J_{k-2}}M_{J_{k-1}}$. Continuing this process, we have that $J = J_0 = M_{J_0}M_{J_1}\cdots M_{J_{k-1}}$. This is a factorization of J into maximal (hence prime) ideals. So R is Dedekind. $\square$

Theorem: (from exercises) Let R be a Dedekind domain with quotient field K. Let L be a finite field extension of K and let S be the integral closure of R in L. Then, S is a Dedekind domain.

1.6 Chapter VI - The Structure of Fields

1.6.1 Section VI.1 - Transcendence Bases

Definition: Let F be a field extension of K and S a subset of F. We say that S is algebraically dependent over K if for some $n \geq 1$, there exists a nonzero polynomial $f \in K[x_1, \ldots, x_n]$ such that $f(s_1, \ldots, s_n) = 0$ for distinct elements $s_1, \ldots, s_n \in S$. We say that S is algebraically independent if S is not algebraically dependent.

Example: If $F = K(x_1, \ldots, x_n)$, then the n variables $x_1, \ldots, x_n$ are algebraically independent.

Theorem VI.1.2: Let F be an extension of K and $\{s_1, \ldots, s_n\}$ a subset of F which is algebraically independent over K. Then,

$$K(s_1, \ldots, s_n) \cong K(x_1, \ldots, x_n).$$

Proof: By the **Universal Mapping Property for Polynomial Rings**, there exists a unique homomorphism

$$\begin{aligned} \varphi : K[x_1, \ldots, x_n] &\longrightarrow K(s_1, \ldots, s_n) \\ x_i &\longmapsto s_i. \end{aligned}$$

By algebraic independence, φ is injective. Since φ is injective, it extends to a unique homomorphism

$$\widehat{\varphi} : K(x_1, \ldots, x_n) \to K(s_1, \ldots, s_n).$$

Observe that $\widehat{\varphi}$ is surjective since $K(s_1, \ldots, s_n)$ is generated over K by the $s_i = \widehat{\varphi}(x_i)$. $\square$

Definition: A transcendence base of F over K is a subset $S \subset F$ which is algebraically independent over K and which is maximal (with respect to set inclusion) among all algebraically independent subsets.

Example: Let $F = K(x)$ and consider $f/g \in F$, where $f, g \in K[x]$ and $g \neq 0$. We claim that the set $\{x, f/g\}$ is algebraically dependent over K. Consider the polynomial $h(y_1, y_2) := g(y_1)y_2 - f(y_1)$. Now

$$h(x, f/g) = g(x)\frac{f(x)}{g(x)} - f(x) = 0$$

and so these two are algebraically dependent. Hence, $\{x\}$ is a transcendence base for $K(x)$ over K.

Theorem VI.1.5: Let F be an extension of K and $S \subset F$ a subset algebraically independent over K and $u \in F \setminus K(S)$. Then, $S \cup \{u\}$ is algebraically independent if and only if u is transcendental over $K(S)$.

Proof: Suppose there exists n and $s_1, \ldots, s_n \in S$, and $f(x_1, \ldots, x_n, x_{n+1}) \in K[x_1, \ldots, x_n, x_{n+1}]$ such that $f(s_1, \ldots, s_n, u) = 0$. Then, define

$$g(x_{n+1}) := f(s_1, \ldots, s_n, x_{n+1}) \in K(S)[x_{n+1}].$$

It's clear as claimed that g is a polynomial in one variable with coefficients in $K(S)$, and that $g(u) = 0$. Since u is transcendental over $K(S)$, we have that g is the zero polynomial. Let

$$g(x_{n+1}) = \sum h_i(s_1, \ldots, s_n)x_{n+1}^i.$$

From this, it's clear that $h_i(s_1, \ldots, s_n) = 0$ for all i and thus $h_i(x_i, \ldots, x_n) = 0$ for all i. Thus,

$$f(x_1, \ldots, x_n, x_{n+1}) = \sum h_i(x_1, \ldots, x_n)x_{n+1}^i = 0$$

and so f is the zero polynomial. Hence, $S \cup \{u\}$ is algebraically independent.

Conversely, assume $S \cup \{u\}$ is algebraically independent. Suppose $h(u) = 0$ for some $h \in K(S)[x]$. Then, we can write h as

$$h(s_1, \ldots, s_n) = \sum_{i=0}^{m} \frac{f_i(s_1, \ldots, s_n)}{f_i(s_1, \ldots, s_n)} x^i.$$

If we clear the denominators, then we get that

$$H \in K[S][x]$$

such that $H(u) = 0$, where the coefficients of H are polynomials in the elememts $s_1, \ldots, s_n$. Then, we have a relation of algebraic dependence of $S \cup \{u\}$, which is a contradiction. Therefore, u is transcendental over $K(S)$. $\square$

Corollary VI.1.6: Let F be an extension of K and $S \subset F$ algebraically independent over K. Then, S is a transcendence basis for F over K if and only if F is algebraic over $K(S)$.

Definition: We say that F is purely transcendental over K if and only if $F = K(S)$ for some algebraically independent set S.

Corollary VI.1.7: If F is an extension of K and for some $X \subseteq F$ we have that F is algebraic over $K(X)$, then X contains a transcendental basis of F over K.

Theorem VI.1.8: Let F be an extension of K. If S is a finite transcendence basis of F over K, then every transcendence basis of F over K has the same size as S.

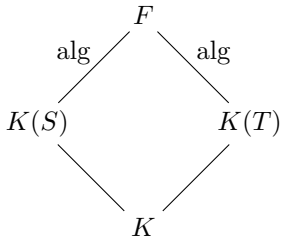
Proof: Let $S = \{s_1, \ldots, s_n\}$ and let T be another transcendence basis. We claim that there exists $t_1 \in T$ such that t_1 is transcendental over $K(s_2, \ldots, s_n)$. If every $t \in T$ is algebraic over $K(s_2, \ldots, s_n)$, then $K(T)$ is algebraic over $K(s_2, \ldots, s_n)$, and so F is algebraic over $K(s_2, \ldots, s_n)$, which is a contradiction. Hence such a t_1 exists.

Now we check that $\{t_1, s_2, \ldots, s_n\}$ is a transcendence basis of F over K. We need to show that s_1 is algebraic over $K(t_1, s_2, \ldots, s_n)$. Suppose not. Then, $\{s_1, t_1, s_2, \ldots, s_n\}$ is algebraically independent, which is a contradiction. Hence, $K(t_1, s_1, s_2, \ldots, s_n)$ is algebraic over $K(t_1, s_2, \ldots, s_n)$. Hence, F is algebraic over $K(t_1, s_2, \ldots, s_n)$. So, the check is complete.

Repeating this process, we find that $T = \{t_1, \ldots, t_n\}$ and thus they have the same size.

Theorem VI.1.9: Let F be an extension of K and let S be a transcendental basis of infinite cardinality. Then, every transcendence basis of F over K has the same cardinality of S.

Proof: Let T be another transcendence basis. T is also infinite by the previous theorem. Now, we have the diagram



Let $s \in S$. Then, s is algebraic over $K(T)$. So there exists a finite subset $T_s \subset T$ such that s is algebraic over $K(T_s)$. Choose T_s for each $s \in S$. We now cliam that $\cup(T_s) \subset T$.

We check that F is algebraic over $K(\cup(T_s))$. By construction, $K(S)$ is algebraic over $K(\cup(T_s))$ and F is algebraic over $K(S)$. So, the check is true. So, $\cup(T_s)$ is a transcendence basis. Hence $\cup(T_s) = T$.

Finally, we check that $|\cup(T_s)| \leq |S|$. $\square$

Definition: Let F be an extension of K. Then, the transcendence degree $\mathrm{TrDeg}\left[F : K\right]$ is the cardinality of a transcendence basis for F over K.

Theorem VI.1.11: If $K \subset F \subset E$, then $\mathrm{TrDeg}\left[E : K\right] = \mathrm{TrDeg}\left[E : F\right] + \mathrm{TrDeg}\left[F : K\right]$.

Theorem VI.1.12: Let F_1, F_2 be algebraically closed extensions of K_1, K_2 respectively. If $\mathrm{TrDeg}\left[F_1 : K_1\right] = \mathrm{TrDeg}\left[F_2 : K_2\right]$ then any isomorphism of K_1 to K_2 extends to an isomorphism $F_1 \cong F_2$.

1.7 Chapter VIII - Commutative Rings and Modules (Again)

1.7.1 Section VIII.7 - The Hilbert Nullstellensatz

Definition: Let K be a field. Let F be an algebraically closed extension of K. Let $S \subseteq K[x_1, \ldots, x_n]$. Consider the set

$$V(S) := \{(a_1, \ldots, a_n) \in F^n \mid f(a_1, \ldots, a_n) = 0,\ \forall f \in S\}.$$

Subsets of F^n of form $V(S)$ for $S \subseteq K[x_1, \ldots, x_n]$ are called K-algebraic sets. They are also sometimes called affine K-varieties. Note that $V(S) = V(I)$ where I is the ideal generated by S.

Remark: Now, let Y be a subset of F^n and set

$$J(Y) = \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots, a_n) \in Y\}.$$

Observe that $J(Y)$ is an ideal.

Lemma VIII.7.1: Let F be an algebraically closed extension of K, and let $S, T \subseteq K[x_1, \ldots, x_n]$ and let $X, Y \subseteq F^n$. Then,

(i) $V(K[x,1 \ldots, x_n]) = \emptyset$; $J(F^n) = \{0\}$; $J(\emptyset) = K[x_1, \ldots, x_n]$.

(ii) If $S \subseteq T$, then $V(T) \subseteq V(S)$. If $X \subseteq Y$, then $J(Y) \subseteq J(X)$.

(iii) $S \subseteq J(V(S))$; $Y \subseteq V(J(Y))$.

(iv) $V(S) = V(J(V(S)))$; $J(Y) = J(V(J(X)))$.

Remark: Note the similarlity between the above lemma, and the properties of the Galois correspondence between subgroups of the Galois group and intermediate field extensions.

Lemma VIII.7.2: (Noether Normalization Lemma) Let R be an integral domain which is a finitely generated ring extension of a field K (i.e., a finitely generated K-algebra). Let $r := \text{TrDeg}\left[F : K\right]$, where $F = \text{frac}(R)$. Then, there exists an algebraically independent subset $\{t_1, \ldots, t_r\}$ of R such that R is integral over $K[t_1, \ldots, t_r]$.

Proof: Suppose $R = K[u_1, \ldots, u_n]$. Then, $F = K(u_1, \ldots, u_n)$. If $\{u_1, \ldots, u_n\}$ is algebraically independent, then we're done. So, assume that $\{u_1, \ldots, u_n\}$ is algebraically dependent. Then,

$$\sum_{(i_1, \ldots, i_n) \in I} k_{i_1, \ldots, i_n} u_1^{i_1} u_2^{i_2} \cdots u_n^{i_n} = 0,$$

for nonzero $k_{i_1, \ldots, i_n} \in K$. Note that I is finite.

Let $c \in \mathbb{N}$ be greater than all i_k occuring as an entry of all elements of I. If $(i_1, \ldots, i_n), (j_1, \ldots, j_n) \in I$, and if

$$i_1 + ci_2 + c^2 i_3 + \cdots + c^{n-1} i_n = j_1 + cj_2 + c^2 j_3 + \cdots + c^{n-1} j_n$$

then, $c \mid i_1 - j_1$, and by our choice of c we must actually have that $i_1 = j_1$. Therefore,

$$i_2 + ci_3 + \cdots + c^{n-2} i_n = j_2 + cj_3 + \cdots + c^{n-2} j_n,$$

and by the same reasoning we now have $i_2 = j_2$, etc.

Thus, the numbers $i_1 + ci_2 + \cdots + c^{n-1} i_n$ for $(i_1, \ldots, i_n) \in I$ are all distinct positive integers. So, there exists a unique tuple $(j_1, \ldots, j_n) \in I$ such that $j_1 + j_2 c + \cdots + j_n c^{n-1}$ is maximum.

Define v_i for $2 \leq i \leq n$ by $u_2 = v_2 + u_1^c$, $u_3 = v_3 + u_1^{c^2}$, ..., $u_n = v_n + u_1^{c^{n-1}}$. Now,

$$k_{j_1, \ldots, j_n} u_1^{j_1 + j_2 c + \cdots + j_n c^{n-1}} + f(u_1, v_2, \ldots, v_n) = 0$$

where $\deg_{u_1}(f) < j_1 + j_2 c + \cdots + j_n c^{n-1}$.

Dividing by $k_{j_1,\ldots,j_n}$ gives a monic polynomial in $K[v_2,\ldots,v_n][x]$ satisfied by u_1. Now, $R = K[u_1,\ldots,u_n] = K[u_1,v_2,\ldots,v_n]$ and u_1 is integral over $K[v_2,\ldots,v_n]$. Thus, R is integral over $K[v_2,\ldots,v_n]$. If $\{v_2,\ldots,v_n\}$ is algebrically independent, then we're done. Otherwise, repeat the previous step. □

Lemma VIII.7.3:(Weak Nullstellensatz) Let F be an algebraically closed extension of K and let I be a proper ideal of $K[x_1,\ldots,x_n]$. Then,

$$V(I) := \{(a_1,\ldots,a_n) \in F^n \mid f(a_1,\ldots,a_n) = 0,\ \ \forall f \in I\}$$

is not empty.

Proof: First recall that if $I \subseteq J$, then $V(J) \subseteq V(I)$. To prove that $V(I)$ is nonempty, we will show that $V(J)$ is nonempty. So, we can assume that I is a maximal ideal of $K[x_1,\ldots,x_n]$. Therefore, $K[x_1,\ldots,x_n]/I$ is a field, and we can consider the maps:

$$K[x_1,\ldots,x_n] \longrightarrow \overbrace{K[x_1,\ldots,x_n]/I}^{=R} \supset K \subset F$$

Therefore, there exists a field homomorphism from R to F. (By Noetherian normalization, there exist $t_1,\ldots,t_r \in R$ algebraically independent such that R is integral over $K[t_1,\ldots,t_r]$. But R is a field, ie $r = 0$, thus R is algebraic.) Let φ be the induced homomorphism from $K[x_1,\ldots,x_n]$ to F.

Let $f \in K[x_1,\ldots,x_n]$. Then, $\varphi(f(x_1,\ldots,x_n)) = f(\varphi(x_1),\ldots,\varphi(x_n)$. If $f \in I$, then f maps to 0 in R. Hence $0 = f(\varphi(x_1),\ldots,\varphi(x_n))$. Thus,

$$(\varphi(x_1),\ldots,\varphi(x_n)) \in F^n$$

is an element of $V(I)$. So, $V(I)$ is nonempty. □

Theorem VIII.7.4: (Hilbert Nullstellensatz) Let F be an algebraically closed extension of K and I a proper ideal of $K[x_1,\ldots,x_n]$. Then, $J(V(I)) = \mathrm{rad}(I)$.

Proof: Observe that $\mathrm{rad}(I) \subseteq J(V(I))$ from definitions and the fact that in a field, $a^m = 0$ if and only if $a = 0$.

Conversely, let $f \in J(V(I))$, and assume without loss of generality that $f \neq 0$. Regard $K[x_1,\ldots,x_n]$ as a subring of $K[x_1,\ldots,x_n,y]$. Let L be the ideal of $K[x_1,\ldots,x_n,y]$ generated by I and $yf - I$.

If $(a_1,\ldots,a_n,b)$ is a zero of L in F^{n+1}, then $(a_1,\ldots,a_n) \in V(I)$. But,

$$(yf-1)(a_1,\ldots,a_n,b) = b\underbrace{f(a_1,\ldots,a_n)}_{=0} - 1 = -1.$$

This shows that L has no common zeros in F^{n+1}. By **Weak Nullstellensatz**, we have that $L = K[x_1,\ldots,x_n,y]$, and so we can write

$$1 = \left(\sum_{i=1}^{t-1} g_i f_i\right) + g_t(yf-1)$$

where $f_i \in I$. The g_i are polynomials in $n+1$ variables (in $K[x_1,\ldots,x_n,y]$).

Now consider the evaluation homomorphism

$$K[x_1,\ldots,x_n,y] \longrightarrow K(x_1,\ldots,x_n)$$

by choosing the mapping $x_i \mapsto x_i$ and $y \mapsto \frac{1}{f}$. Applying this to the equation for 1 above, we get

$$1 = \sum_{i=1}^{t-1} g_i(x_1, \ldots, x_n, \frac{1}{f}) f_i(x_1, \ldots, x_n).$$

Let f^m be the highest power of f occuring in any denominator of any g_i. Then,

$$f^m = \sum_{i=1}^{t-1} \underbrace{g_i f^m}_{\in K[x_1,\ldots,x_n]} \underbrace{f_i}_{\in I}.$$

Therefore, $f \in \operatorname{rad}(I)$. $\square$

Remark: Let K be a field and let F be an algebraically closed extension of K. Each $f \in K[x_1, \ldots, x_n]$ defines a function from F^n to F by substitution. If $V = V(I)$, then $f\big|_V$ is a function on V. We have the map

$$\Gamma : K[x_1, \ldots, x_n] \xrightarrow{\text{restriction}} \big\{F\text{-valued functions on } V\big\}.$$

The image $\Gamma(V)$ is called the ring of regular functions. The kernel $\operatorname{Ker}(\Gamma)$ is defined to be $J(V(I))$, and so

$$\Gamma(V) \cong K[x_1, \ldots, x_n]/J(V(I)) = K[x_1, \ldots, x_n]/\operatorname{rad}(I).$$

Γ has the properties:

(1) $\Gamma(V)$ is a finitely generated K-algebra.

(2) $\Gamma(V)$ has no nilpotent elements. (This condition is sometimes called reduced.)

Remark: If the reader is interested in more of this type of material, they should investigate the Zariski Topology.

1.8 Chapter IX - The Structure of Rings

1.8.1 Section IX.1 - Simple And Primitive Rings

Definition: A left module A over a ring R is called simple or irreducible if $RA \neq 0$ and A has no proper subgroups. We call a ring R simple if $R^2 \neq 0$ and R has no proper (two-sided) ideals.

Remark: If R has a 1, then for any maximal left ideal L (which exists by Zorn's Lemma), R/L is a simple module.

Theorem: (Schur's Lemma) Suppose R is a ring and A is a simple R-module. Then, $\text{End}_R(A)$ is a division ring. Recall that

$$\text{End}_R(A) := \varphi \in \text{End}_{\mathbb{Z}}(A) \mid r(\varphi(a)) = \varphi(ra), \ \ \forall r \in R, a \in A\}.$$

Remark: We can consider the left modules ${}_RA$ and consequently ${}_{\text{End}_R(A)}A$. In fact, since any module over a division ring is free (i.e., a vector space), we have that ${}_{\text{End}_R(A)}A$ is a vector space. This is the idea of double centralizers.

Proof: We show that every nonzero element of $\text{End}_R(A)$ is invertible. Let $\varphi \in \text{End}_R(A)$ be nonzero. Since $\text{Ker}(\varphi)$ is a submodule of A, and since A is simple and $\text{Ker}(\varphi) \neq A$, we have that $\text{Ker}(\varphi) = \{0\}$. Hence, φ is injective. Similarly, $\text{Im}(\varphi)$ is a submodule of A and it's nontrivial, so $\text{Im}(\varphi) = A$. So, φ is a bijection, and so $\varphi^{-1} \in \text{End}_R(A)$, as long as φ^{-1} is still an R-module homomorphism, which we verify now.

We want to check that $\varphi^{-1}(ra) = r\varphi^{-1}(a)$. Let $a \in A$ and let $b = \varphi^{-1}(a)$, so that $\varphi(b) = a$. Now,

$$\varphi^{-1}(ra) = \varphi^{-1}(r\varphi(b)) = \varphi^{-1}(\varphi(rb)) = rb = r\varphi^{-1}(a).$$

Hence $\varphi^{-1} \in \text{End}_R(A)$. Therefore, $\text{End}_R(A)$ is a division ring. $\square$

Remark: The converse to Schur's Lemma is false. For example, let F be a field and let R be the ring

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in F \right\}.$$

Let

$$A := F^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x, y \in F \right\}.$$

Now,

$$A_1 := \left\{ \begin{pmatrix} z \\ 0 \end{pmatrix} \mid z \in F \right\}.$$

is a nonzero proper submodule of A and so is not simple. However, R acts on A by left matrix multiplication, and so $\text{End}_R(A) \cong F$, which is a division ring (since it's a field).

Definition: A left ideal I in a ring R is regular if there exists $e \in R$ such that $r - re \in I$ for every $r \in R$. A right ideal J is regular if there exists $e \in R$ such that for all $r \in R$ we have that $r - er \in J$. Note that rings with unity are all regular, by choosing $e = 1$.

Theorem IX.1.3: A left module A over a ring R is simple if and only if there exists a left maximal regular ideal I such that $A \cong R/I$ as R-modules.

Proof: Let A be a simple module. Then, $RA \neq 0$ and so there exists $a \in A$ such that $Ra \neq 0$. Since Ra is a submodule of A, we must have that $Ra = A$. Thus the map $R \to Ra = A$ defined by $r \mapsto ra$ is

an R-module homomorphism. Let I be the kernel of this map, so that I Is a left ideal and $R/I \cong A$. Since $Ra = a$, there exists $e \in R$ such that $ea = a$. Then, for any $r \in R$, we have that $ra = rea$ and so $(r - re)a = 0$. Thus, $r - re \in I$. Hence I is a left maximal regular ideal.

Conversely, suppose that I is a left maximal regular ideal of R. Then, R/I is an R-module. Pick e such that $r - re \in I$ for all $r \in R$. Now, we check that $R(R/I) \neq 0$. Suppose $r(R/I) = 0$ for all $r \in R$. Then, $0 = r(e + I) = re + I = r + I$. Hence, $R \subseteq I$, which is a contradiction. Hence R/I is simple. $\square$

Definition: Let R be ring and let A be a (left) R-module. Then, $\mathrm{Ann}_R(A)$ is an ideal, namely the kernel of $\rho : R \to \mathrm{End}_{\mathbb{Z}}(A)$. We say that A is a faithful module (or that ρ is a faithful action) if $\mathrm{Ann}_R(A) = 0$. We say that a ring is primitive if it has a faithful, simple module.

Remark: Consider a ring $R \subseteq \mathrm{End}_{\mathbb{Z}}(A)$, and note that then $\mathrm{End}_R(A) =: D \subseteq \mathrm{End}_{\mathbb{Z}}(A)$, and D is a division ring. Now, A can be viewed in one of two ways: either as an R-module, with $D = \mathrm{End}_R(A)$, or as a D-module, with $R \subseteq \mathrm{End}_D(A)$. While equality in this last containment may not be true, we will see that in some sense R is at least a large part of $\mathrm{End}_D(A)$.

Definition: Let V be a (left) vector space over a division ring D. A subring R of $\mathrm{End}_D(V)$ is called a dense ring of endomorphisms of V if, for every positive integer n and every linearly independent subset $\{u_1, \ldots, u_n\}$ of V and every arbitrary sequence $v_1, \ldots, v_n$, there exists $\theta \in R$ such that $\theta(u_i) = v_i$.

Theorem IX.1.9: Let R be a dense ring of endomorphisms of a left (resp. right) vector space V over a division ring D. Then, R is left (resp. right) Artinian if and only if $\dim_D(V)$ is finite, in which case $R = \mathrm{End}_D(V)$

Proof: We prove the left case. The right case is analogous. Let $R \subseteq \mathrm{End}_{\mathbb{Z}}(V)$ and suppose that R is left Artinian. Assume toward a contradiction that $\dim(V)$ is infinite. Then, there exists an infinite linearly independent set $\{u_1, u_2, \ldots\}$. We can view V as a left R-module. For each n, let $I_n := \mathrm{Ann}_R(\{u_1, \ldots, u_n\})$. Then, I_n is a left ideal and $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$. These inclusions must be proper, so this contradicts the assumption that R is Artinian. Hence $\dim(V)$ is finite.

Conversely, if $\dim_D(V)$ is finite, then we observe that the only dense ring of endomorphisms is $\mathrm{End}_D(V)$. So, $R = \mathrm{End}_D(V) \cong \mathrm{Mat}_n(D)$ for $n = \dim_D(V)$. We proved previously that $\mathrm{Math}_n(D)$ is left (and right) Artinian, because it has a composition series. $\square$

Lemma IX.1.11: Let A be a simple R-module for any ring R. Let $D := \mathrm{End}_R(A)$ and view A as a D-vector space. If V is a finite dimensional D-subspace of A and $a \in A \setminus V$, then there exists $r \in R$ such that $ra \neq 0$ and $rV = 0$.

Proof: (by induction on $\dim_D(V)$) If $\dim_D(V) = 0$, then $V = \{0\}$ and $a \neq 0$. Since A is simple, by a remark following the definition of a simple module in Hungerford, we have that $Ra = A$ and so there exists $r \in R$ such that $ra \neq 0$.

Now, assume true for $n - 1$. Firstly, if W is an $(n-1)$-dimensional subspace and $u \in A \setminus W$, then there exists $r \in R$ such that $rW = 0$ and $ra \neq 0$. Secondly, if W is an $(n-1)$-dimensional subspace and $I := \mathrm{Ann}_R(W)$ is a left ideal, then if $v \in A$ and $rv = 0$ for all $r \in I$, it follows that $VinW$.

Let V be an n-dimensional subspace and let $a \in A \setminus V$. Let $\{v_1, \ldots, v_n\}$ be a basis of V. Let $W := \mathrm{Span}\{v_1, \ldots, v_{n-1}\}$. Then, $V = W \oplus Dv_n$. Set $I := \mathrm{Ann}_V(W)$. Then, there exists $r \in I$ such that $rv_n \neq 0$. Then, Iv_n is an R-submodule of A since I is a left ideal. So, $Iv_n \neq 0$ and hence $Iv_n = A$.

We want $r \in R$ such that $rV = 0$ with $ra \neq 0$. Such an r must be in I. If no such r exists, then define $\theta : A \to A$ as follows: for $rv_n \in Iv_n = A$, set $\theta(rv_n) = ra$. To see that θ is well-defined, if $r_1v_n = r_2v_n$ for $r_i \in I$, then $(r_1 - r_2)v_n = 0$. Hence $r_1 - r_2 \in \mathrm{Ann}(V)$. Thus, $(r_1 - r_2)a = 0$ and so $r_1a = r_2a$. Hence, well-defined.

Note that $\theta \in \mathrm{End}_R(A) =: D$. For all $r \in I$ we have that

$$0 = \theta(rv_n) - ra = r\theta(v_n) - ra = r(\theta(v_n) - a).$$

Hence by our "secondly" remark above, it follows that $\theta(v_n) - a \in W$ and so $a = \theta(v_n) - (\theta(v_n) - a) \in Dv_n + W = V$, which is a contradiction. Hence the lemma follows. □

Theorem IX.1.12: (Jacobson Density Theorem) Let R be a primitive ring with faithful simple module A. Consider A as a vector space over $D := \mathrm{End}_R(A)$. Then, R is isomorphic to a dense ring of endomorphisms of the D-vector space A.

Proof: For $r \in R$, define $\alpha_r : A \to A$ to be the map $a \mapsto ra$, so $\alpha_r \in \mathrm{End}_D(A)$. Now define $\alpha : R \to \mathrm{End}_D(A)$ by $r \mapsto \alpha_r$.

Let $\{u_1, \ldots, u_n\}$ be a linearly independent set in A. Let $v_1, \ldots, v_n$ be an arbitrary sequence of n elements. We want to find $r \in R$ such that $\alpha_r(u_i) := ru_i = v_i$ for all i. By the previous **Lemma** we have for each i an element $r_i \in R$ such that $r_i u_i \neq 0$ and $r_i u_j = 0$ for all $j \neq i$.

Also by the **Lemma**, for all i there exists s_i such that $s_i r_i u_i \neq 0$. Then, $Rr_i u_i \neq 0$, so $Rr_i v_i = A$ for all i. So, for all i, there exists $t_i \in R$ such that $t_i r_i u_i = v_i$. Note that $t_i r_i u_j = 0$ for all $j \neq i$.

Let $r = \sum_i t_i r_i$. Now after checking that this r works, the theorem is complete. □

Remark: Let A, D be as above. If $n := \dim_D(A) < \infty$, then $\mathrm{End}_D(A) \cong \mathrm{Mat}_n(D)$ is a simple Artinian ring. If S is a dense subring of $\mathrm{Mat}_n(D)$, then $S = \mathrm{Mat}_n(D)$.

Corollary IX.1.13: If R is a primitive ring, then either $R \cong \mathrm{Mat}_n(D)$ for some $n \in \mathbb{N}$ and some division ring D, or else for all $n \in \mathbb{N}$, there exists a subring R_n of R and a surjective homomorphism $R_n \to \mathrm{Mat}_n(D)$.

Proof: Let M be a faithful simple R-module. If $\dim_D(M) =: n < \infty$, then $R \cong \mathrm{Mat}_n(D)$. Assume $\dim_D(M) = \infty$. Let $m_1, m_2, \ldots$ be an infinite linearly independent sequence of elements. Set $R_n := \{r \in R \mid rM_n \subseteq M)n\}$, where $M_n := \mathrm{span}_D(\{m_1, \ldots, m_n\})$.

Then, since R acts densely on M, it follows that R_n acts densely on M_n, and so we have a homomorphism $R_n \twoheadrightarrow \mathrm{End}_D(M_n) \cong \mathrm{Mat}_n(D)$. □

Theorem IX.1.14: (Wedderburn-Artin) The following conditions on a left Artinian ring are equivalent.

(i) R is simple.

(ii) R is primitive.

(iii) R is isomorphic to $\mathrm{End}_D(V)$ for some D-vector space V.

(iv) $R \cong \mathrm{Mat}_n(D)$ for some n and D.

Proof:

(i) $\Longrightarrow$ (ii) Let I be a minimal left ideal. Then, $\mathrm{Ann}_R(I)$ is an ideal, and so it must be zero or R. If $\mathrm{Ann}_R(I) = R$, then $RI = 0$ and so $\{r \in R \mid Rr = 0\} \neq 0$. But, this set is an ideal and hence must be R, but since $R^2 \neq 0$, this is a contradiction. Thus, $\mathrm{Ann}_R(I) = 0$ and $RI \neq 0$, so I is a faithful simple module and R is primitive.

See Hungerford for other equivalences. □

Lemma IX.1.15: Let V be a finite dimensional vector space over a division ring D. If A and B are simple faithful modules over the endomorphism ring $R = \mathrm{Hom}_D(V, V)$, then A and B are isomorphic R-modules.

Proof: Let I be a minimal left ideal of R. Then, A is faithful since R is simple, so $IA \neq 0$. Then, there exists $a \in A$ such that $Ia \neq 0$. But, Ia is an R-submodule of A, and hence equal to A.

We must check that $I \to Ia(= A)$ given by $r \mapsto ra$ is a nonzero R-module homomorphism, necessarily an isomorphism, since I and A are simple. $\square$

Lemma IX.1.16: Let V be a D-division space and $R = \mathrm{End}_D(V)$. Suppose that $g : V \to V$ is a homomorphism of abelian groups such that $gr = rg$ for all $r \in R$ (i.e., g is an R-endomorphism). Then, there exists $d \in D$ such that for all $v \in V$, we have $gv = dv$.

Let u be a nonzero element of V. Show that u and $g(u)$ are linearly dependent over D. If $\dim_D(V) = 1$, then everything works out. So, now suppose that $\dim_D(V) \geq 2$ and that $\{u, g(u)\}$ is a linearly independent set. Then, there exists $r \in R(= \mathrm{End}_D(V))$ such that $ru = 0$ and $rg(u) \neq 0$. But, we have that

$$r(g(u)) - g(r(u)) = 0$$

which yields a contradiction. Therefore there exists $d \in D$ such that $g(u) = du$. Now, if $v \in V$ then by density we can choose $s \in R$ such that $s(u) = v$. Now,

$$g(v) = g(su) = sg(u) = s(du) = d(su) = dv. \ \square$$

Proposition IX.1.17: For $i = 1, 2$, let V_i be a vector space of finite dimension n_i over the division ring D_i. Then,

(i) If there is an isomorphism of rings $\mathrm{Hom}_{D_1}(V_1, V_1) \cong \mathrm{Hom}_{D_2}(V_2, V_2)$, then $\dim_{D_1}(V_1) = \dim_{D_2}(V_2)$ and $D_1 \cong D_2$.

(ii) If there is an isomorphism of rings $\mathrm{Mat}_{n_1}(D_1) \cong \mathrm{Mat}_{n_2}(D_2)$, then $n_1 = n_2$ and D_1 is isomorphic to D_2.

Recall: $\mathrm{End}_D(M) \cong \mathrm{Mat}_n(D^{\mathrm{opp}})$ for any D-vector space M.

Example: Let ${}_DD$ be the 1-dimensional left D-vector space. Let $\varphi \in \mathrm{End}_D({}_DD)$. Set $a := \varphi(1)$. Then, for any $d \in {}_DD$, we have that $\varphi(d) = \varphi(d, 1) = d\varphi(1) = da$. Hence, φ is right multiplication by a.

Let $\varphi, \varphi' \in \mathrm{End}_D({}_DD)$. Then, there exists a and $a' \in D$ such that $\varphi_a(x) = xa$ and $\varphi_{a'} = xa'$ for all $x \in D$. Then, $(\varphi_a \circ \varphi_{a'})(x) = \varphi_a(\varphi_{a'}(x)) = \varphi_a(xa') = xa'a$. Thus, $\varphi \circ \varphi'$ is multiplication by $a'a$. This tells us that $\mathrm{End}_D({}_DD) \cong D^{\mathrm{opp}}$.

1.8.2 Section IX.2 - The Jacobson Radical

Definition: An ideal I of a ring R is left primitive if R/I is a (left) primitive ring. Note that we're not saying that I is a left ideal. We have an analogous definition of a right primitive ideal.

Definition: An element $a \in R$ is left quasi-regular if there exists $r \in R$ such that $ra + r + a = 0$. We have an analogous definition of a right quasi-regular element of R.

Definition: An ideal I is called left quasi-regular if every element of I is left quasi-regular. Again we have the analogous definition for a right quasi-regular ideal.

Recall: A left ideal I is regular if there exists $e \in R$ such that for all $r \in R$ we have $r - re \in I$.

Lemma IX.2.4: If $I \neq R$ is a regular left ideal of R, then I is contained in a maximal left ideal which is regular.

> **Proof:** Since I is regular, there exists $e \in R$ such that for all $r \in R$ we have $r - re \in I$. Hence, any left ideal J containing I is also regular.
>
> Let $\mathscr{S}$ be the set of all ideals L such that $I \subseteq L \neq R$, ordered by inclusion. Write $\mathscr{S}$ as $\{I_i\}_{i \in \mathscr{C}}$. Define $K := \cup(I_i)$. This makes K a left ideal. We claim that K is proper. If not, then $e \in K$, and so there exists i such that $e \in I_i$. But then $r - re \in I \subseteq I_i$ for all r, i.e., $re \in I_i$ for all r. Therefore, $I_i = R$, which is a contradiction. $\square$

Lemma IX.2.5: Let K be the intersection of all regular maximal left ideals. Then, K is a left quasi-regular left ideal.

> **Proof:** Let K be a left ideal. Let $a \in K$. Define $T := \{r + ra \mid r \in R\}$. We claim that $T = R$. If this is true, then $-a \in T$ and so there exists r such that $r + ra = -a$, i.e., $ra + r + a = 0$, which makes a left quasi-regular.
>
> So, we now show that $T = R$ for every $a \in K$. T is a left ideal and is regular (take $e = -a$). Assume $T \neq R$. So, $T \subseteq I_0$, where I_0 is a regular maximal left ideal. Then, $a \in K \subseteq I_0$, so $ra \in I_0$ for all $r \in R$. Since $r + ra \in T \subseteq I_0$, we get that $r \in I_0$, which is a contradiction. This completes the proof. $\square$

Lemma IX.2.6: Let R be a ring with a simple left module. If I is a left quasi-regular left ideal, then $I \subseteq$ [the intersection of all simple left modules].

> **Proof:** Suppose not. Then, there exists a simple module B with $IB \neq 0$. So, $b \in B$ and $Ib \neq 0$. Hence, $Ib = B$, since Ib is a submodule. Thus, there exists $a \in I$ such that $ab = -b$. Since I is left quasi-regular and $a \in I$, there exists $r \in R$ such that $r + a + ra = 0$.
>
> Calculating,
>
> $$\begin{aligned} 0 &= 0 \cdot b \\ &= (r + a + ra)b \\ &= rb + ab + rab \\ &= rb - b + r(-b) \\ &= -b. \end{aligned}$$
>
> This is a contradiction, since $b \neq 0$. Thus, every left quasi-regular left ideal is contained in the intersection of all annihilators of simple left modules. $\square$

Lemma IX.2.7: An ideal P of R is left primitive if and only if P is the annihilator of a simple left R-module.

Proof: See book.

Lemma IX.2.8: If I is a left ideal and I is left quasi-regular, then I is right quasi-regular.

Proof: Let $a \in I$. Then, there exists $r \in R$ such that $r + a + ra = 0$ and so $r = -a - ra \in I$. Now, there exists s such that $s + r + sr = 0$. Thus, s is right quasi-regular.

Define $\circ$ by $x \circ y := x + y + xy$. Note that $\circ$ is associative. Then,

$$a = 0 \circ a = (s \circ r) \circ a = s \circ (r \circ a) = s \circ 0 = s. \ \square$$

Theorem IX.2.3: Let R be a ring. Then there exists an ideal $J(R)$ such that

(i) $J(R)$ is the intersection of all the left annihilators of simple left R-modules.

(ii) $J(R)$ is the intersection of all regular maximal left ideals.

(iii) $J(R)$ is the intersection of all left primitive ideals.

(iv) $J(R)$ is a left quasi-regular left ideal which contains every left quasi-regular left ideal.

(v) The properties in (i)-(iv) hold when "left" is replaced by "right".

The ideal $J(R)$ is called the Jacobson radical.

Proof: (See book for more details.) Define $J(R)$ to be the intersection all annihilators of simple left R-modules. If $J(R) = R$, then (ii), (iii), and (iv) hold. Now assume $J(R) \neq R$. Then, by **Lemma IX.2.7**, (iii) holds immediately.

To see (ii), define K to be the intersection of all regular maximal left ideals of R. By **Lemmas IX.2.5 & IX.2.6**, we have that $K \subseteq J(R)$, so it remains to prove $J(R) \subseteq K$. Let $c \in J(R)$. By **Theorem IX.1.3**, $J(R)$ is the intersection of all left annihilators of the quotients R/I, where I runs over all regular maximal left ideals of R. For each regular maximal ideal I there exists $e \in R$ such that $c - ce \in I$. Since $c \in \mathrm{Ann}_R(R/I)$, we have that $cr \in I$ for all $r \in R$, and in particular $ce \in I$. Hence, $c \in I$ for every regular maximal ideal I. Thus, $J(R) \subseteq I = K$. Therefore, $J(R) = K$.

For (iv) observe that $J(R)$ is a left quasi-regular left ideal by (ii) and **Lemma IX.2.5**. $J(R)$ contains every left quasi-regular left ideal by **Lemma IX.2.6**.

For (v), see book. $\square$

Remark: In a commutative ring with 1, we have that

$$\bigcap \{\text{maximal ideals}\} = J(R) \supset N(R) = \bigcap \{\text{prime ideals}\}.$$

Recall that $N(R)$ is the nilradical of R.

Example: Let $R = \mathbb{Z}$. Then, $J(R) = \{0\} = N(R)$.

Definition: A ring R is called semisimple if $J(R) = 0$.

Theorem IX.2.10: Let R be a ring.

(i) If R is primitive then R is semisimple.

(ii) If R is simple and semisimple, then R is primitive.

(iii) If R is simple, then either R is primitive semisimple or R is a radical ring.

Definition: An element $a \in R$ is called nilpotent if there exists $n \in \mathbb{N}$ such that $a^n = 0$. A (left, right, two-sided) ideal I is nil if every element of I is nilpotent. An ideal I is called nilpotent if there exists $n \in \mathbb{N}$ such that $I^n = \{0\}$. It is clear that nilpotent ideals are nil, but the converse is false.

Theorem IX.2.12: Let R be a ring. Every nil right or left ideal is contained in $J(R)$.

Proof: Nilpotent elements are left or right quasi-regular. Observe that

$$(1+a)^{-1} = \sum_{i=0}^{\infty} (-1)^i a^i,$$

and this sum is actually finite because a is nilpotent. □

Proposition IX.2.13: Let R be a left Artinian ring. Then, $J(R)$ is a nilpotent ideal. Consequently, every nil left or right ideal is nilpotent and $J(R)$ is the unique maximal nilpotent left (or right) ideal of R.

Proof: Set $J := J(R)$. Note that $J \supset J^2 \supset J^3 \supset \cdots$. By the Artinian condition, there exists $k > 0$ such that $J^k = J^i$ for all $i \geq k$. We claim that $J_k = 0$.

Suppose not. Let $S := \{\text{left ideals } I \text{ such that } J^k I \neq 0\}$. Then,

$$J^k J = J^{k+1} = J^k \neq 0,$$

and so $J \in S$. So, $S \neq \emptyset$¿ Thus S has a minimal element I_0 (by the minimality condition). Then $J^k I_0 \neq 0$, and so there exists $a \in I_0$ such that $J^k a \neq 0$.

Therefore, there exists $r \in J^k$ with $ra = a$. Since $-r \in J^k \subset J$, we see that $-r$ is left quasi-regular. So, there exists $s \in R$ such that $s - r - sr = 0$. Now,

$$\begin{aligned} a &= ra \\ &= -(-ra) \\ &= -(-ra + 0) \\ &= -(-ra + sa - sa) \\ &= -(-ra + sa - s(ra)) \\ &= -(-r + s - sr)a \\ &= 0. \end{aligned}$$

This is a contradiction, and so the theorem is proved. □

Remark: Suppose R is a F-algebra, i.e., R has a 1 and has a subring $F \ni 1_R$ in the center of R. Then, any (left, right, two-sided) ideal of R is a vector space over F. If R is finite dimensional as a vector space over F, we say that R is a finite dimensional algebra. In this case, it is clear from considering dimensions that R is left and right Artinian.

Example: If G is a finite group, then FG (the group algebra) is a finite dimensional algebra.

Theorem IX.2.14: If R is a ring, then $R/J(R)$ is semisimple.

Proof: Let $\pi : R \to R/J(R)$ be the natural projection map. Let $\mathscr{C} := \{\text{regular maximal left ideals of } R\}$. If $I \in \mathscr{C}$ then $J(R) \subseteq I$ and $\pi(I)$ is a maximal left ideal of $R/J(R)$. If $e \in R$ such that $r - re \in I$ for all $r \in R$, then $\overline{r} - \overline{re} \in \pi(I)$ for all $\overline{r} \in R/J(R)$, and so $\pi(I)$ is regular.

Let

$$\overline{r} \in \bigcap_{I \in \mathscr{C}} \pi(I) = \bigcap_{I \in \mathscr{C}} I/J(R).$$

Then,

$$r \in \bigcap_{I \in \mathscr{C}} I = J(R).$$

Then,

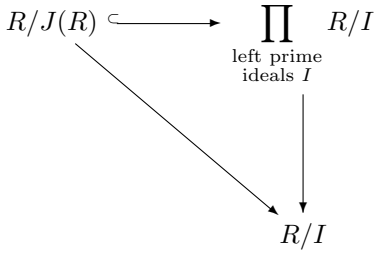
$$J(R/J(R)) = \bigcap \{\text{regular maximal left ideals of } R/J(R)\} \subseteq \bigcap_{I \in \mathscr{C}} \pi(I) = 0.$$

So, $R/J(R)$ is semisimple. $\square$

Remark: Consider a ring R with I a left primitive ideal. Then, R/I is primitive and is isomorphic to a dense ring of automorphisms of a vector space over some division ring. Let $J(R)$ be the intersection of all left primitive ideals. We can consider the map

$$R \longrightarrow \prod_{\substack{\text{left prime} \\ \text{ideals } I}} R/I,$$

which induces the diagram



This map is called the subdirect product.

Theorem: R is simple if and only if R is isomorphic to a subdirect product of primitive rings.

Proof: We have already shown that if $J(R) = 0$ then R is isomorphic to a subdirect product of primitive rings (see the remark above). Conversely, if $R \subseteq \prod R_i$ is a subdirect product of primitive rings, let $\pi_i : R \twoheadrightarrow R_i$ be the i^{th} projection. Then, $\text{Ker}(\pi_i)$ is a left primitive ideal and $J(R) \subseteq \cap(\text{Ker}(\pi_i)) = \{0\}$. Therefore, R is semisimple. $\square$

Lemma IX.2.15: Let R be a ring and let $a \in R$. Then,

(i) If $-a^2$ is left quasi-regular then so is a.

(ii) $a \in J(R)$ if and only if Ra is a left quasi-regular left ideal.

Remark: Recall that we cannot call Ra "the ideal generated by a" because R might not have a 1, in which case $a \notin Ra$.

Proof of (i): Since $-a^2$ is quasi-regular, there exists $r \in R$ such that

$$r + (-a^2) + r(-a^2) = 0.$$

Define $s := r - a - ra$. Now,

$$\begin{aligned} s + a + sa &= r - a - ra + a + (r - a - ra)a \\ &= r - ra + ra - a^2 - ra^2 \\ &= r - a^2 - ra^2 \\ &= 0. \end{aligned}$$

Thus s is the ring element which shows that a is left quasi-regular. $\square$

Proof of (ii): If $a \in J(R)$ then $Ra \subseteq J(R)$, and so Ra is a left quasi-regular left ideal. Conversely, suppose that Ra is a left quasi-regular left ideal. Set $K := \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$. Then, K is a left ideal containing a and Ra. Let $s = ra + na \in K$. Then, $-s^2 = -(ra + na)(ra + na)$ and we see that $-s^2$ is left quasi-regular. Hence so is s by **part (i)**. Therefore, K is left quasi-regular, and thus $K \subseteq J(R)$, i.e., $a \in J(R)$. $\square$

Theorem IX.2.16: If I is an ideal of R (regarded as a ring), then

(i) $J(I) = I \cap J(R)$,

(ii) If R is semisimple then so is every ideal of R,

(iii) $J(R)$ is a radical ring, i.e., $J(J(R)) = J(R)$.

Proof of (i): It's clear that $I \cap J(R)$ is an ideal of I. If $a \in I \cap J(R)$, then a is a left quasi-regular element of R, and so there exists $r \in R$ such that $r + a + ra = 0$. Since $a \in I$ and $ra \in I$ we see that $r \in I$. Therefore, a is actually a left quasi-regular element of I. This tells us that $I \cap J(R)$ is a left quasi-regular left ideal of I, and hence $I \cap J(R) \subseteq J(I)$.

Conversely, assume $a \in J(I)$ and $r \in R$. Then,

$$-(ra)^2 = -(rar)a \in IJ(I) \subseteq J(I).$$

Therefore, $-(ra)^2$ is left quasi-regular in I. By the previous lemma, ra is left quasi-regular in I, and so it is left quasi-regular in R. This yields that the ideal Ra is left quasi-regular in R, and so $a \in J(R)$. Therefore, $J(I) \subseteq I \cap J(R)$. $\square$

Theorem IX.2.17: If R_i for $i \in I$ is a family of rings, then $J(\prod R_I) = \prod(J(R_i))$.

Proof: Let $(a_i)_{i \in I} \in \prod(R_i)$. Then check that this element is left quasi-regular if and only if a_i is left quasi-regular in R_i. Therefore, $\prod(J(R_i))$ is a left quasi-regular ideal of $\prod(R_i)$. So, $\prod(J(R_i)) \subseteq J(\prod(R_i))$. Let $\pi_k : \prod(R_i) \to R_k$ be the canonical projection, and set $I_k = \pi_k(J(\prod(R_i))) \subseteq J(R_k)$. Therefore, $J(\prod(R_i)) \subseteq \prod(J(R_i))$. $\square$

1.8.3 Section IX.3 - Semisimple Rings

Theorem IX.3.3: (Wedderburn-Artin) The following conditions on a ring are equivalent:

(i) R is a nonzero semisimple left Artinian ring.

(ii) R is a direct product of a finite number ideals, each of which is a simple ring isomorphic to the endomorphism ring of a finite dimensional vector space over a division ring.

(iii) There exist division rings $D_1, \ldots, D_t$, and positive integers $n_1, \ldots, n_t$ such that

$$R \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t).$$

Proof: First note that (ii) $\iff$ (iii) is slightly trivial, see Hungerford.

We now prove (i) $\iff$ (ii). For, (ii) $\implies$ (i), recall that

$$J\left(\prod R_i\right) = \prod J(R_i).$$

If the R_i are simple and primitive they are semisimple. So, $J(R) = 0$. Also, $\mathrm{End}_{D_i(V_i)}$ is left Artinian for any vector space V_i over a division ring D_i. Hence

$$\prod_{i=1}^{t} \mathrm{End}_{D_i}(V_i)$$

is also left Artinian.

Now we show the much harder (i) $\implies$ (ii). First observe that

$$0 = J(R) = \bigcap \{\text{left primitive ideals of } R\} = \bigcap_{i \in I} P_i,$$

where $\{P_i \mid i \in I\}$ is the set of left primitive ideals of R. Now,

$$\varphi : R \hookrightarrow \prod_{i \in I} R/P_i$$

by the natural map. Suppose we know that I is a finite set. Well, each R/P_i is simple, and the P_i are maximal ideals, so

$$R^2 + P_i = R$$

since $(R/P_i)^2 \neq 0$, and

$$P_i + P_j = R$$

for all $i \neq j$. So, by the **Chinese Remainder Theorem**, φ is surjective, and so an isomorphism, which would complete the theorem. So, in this step it remains to prove that indeed I is a finite set.

Well, observe that

$$\begin{aligned} R^2 &= (P_1 + P_2)(P_1 + P_3) \\ &= P_1^2 + P_1P_3 + P_2P_1 + P_2P_3 \\ &\subseteq P_1 + P_2P_3 \\ &\subseteq P_1 + P_2 \cap P_3. \end{aligned}$$

So,

$$R = R^2 + P_1 \subseteq P_1 + P_2 \cap P_3.$$

By induction and repeating this process, we have that

$$P_1 + (P_2 \cap \cdots \cap P_n) = R$$

if the P_i are distinct.

Now assume toward a contradiction that I is infinite. Consider

$$P_1 \supset P_1 \cap P_2 \supset P_1 \cap P_2 \cap P_3 \supset \cdots .$$

By DCC, there exists n such that

$$P_1 \cap P_2 \cap \cdots \cap P_n = P_1 \cap P_2 \cap \cdots \cap P_n \cap P_{n+1},$$

i.e.,

$$P_{n+1} \supset P_1 \cap P_2 \cap \cdots \cap P_n.$$

But, but our calculation, we know that

$$R = P_{n+1} + (P_1 \cap \cdots \cap P_n) \subseteq P_{n+1}.$$

This is a contradiction, and so the theorem is complete. □

Corollary IX.3.4:

(i) A semisimple left Artinian ring has an identity.

(ii) A semisimple ring is left Artinian.

(iii) A semisimple left Artinian ring is both left and and right Noetherian.

Definition: An element e of a ring is called an idempotent if and only if $e^2 = e$.

Remark: In the case of a semisimple ring as in the Wedderburn-Artin Theorem, we can write the elements of R in the form

$$(M_1, \ldots, M_t)$$

and so we can find idempotents e_j defined by

$$e_j := (0, \ldots, 0, I_{n_j}, 0, \ldots, 0)$$

where I_{n_j} is in the j^{th} component and is the identity matrix of the correct size.

Corollary IX.3.5: If I is an ideal in a semisimple left Artinian ring R, then $I = Re$ for e an idempotent in the center of R.

Proof: Note that

$$Re_j = \{(0, 0, \ldots, 0, M, 0, \ldots, 0, 0)\}$$

and this is a simple ideal of R. So,

$$I \cap Re_j = \begin{cases} Re_j, & e_j \in I \\ 0, & e_j \notin I \end{cases},$$

since it is an ideal of Re_j. Now, define

$$e := \sum_{e_j \in I} e_j,$$

and

$$e' := \sum_{e_j \notin I} e_j.$$

If $e_k \notin I$, then $Ie_k \in I \cap Re_k = 0$. Then, $Ie' = 0$, and so

$$I = I \cdot 1 = I \left(\sum_{i=1}^{t} e_i \right) = I(e + e') = Ie.$$

This proves the theorem. □

Theorem IX.3.6: Let R be a ring and A be a module. Then, the following are equivalent:

(i) A is a sum of a family of simple submodules.

(ii) A is the (internal) direct sum of a family of simple modules.

(iii) For every nonzero element $a \in A$, we have $Ra \neq 0$. Additionally, every submodule B of A is a direct summand, i.e., there exists a submodule C such that $A = B \oplus C$.

Proof:
(i) $\implies$ (ii): Suppose A is generated by $\{B_i \mid i \in I\}$, a family of simple submodules. Consider subsets J of I such that $\sum_{j \in J} B_j$ is direct.

By **Zorn's Lemma**, there exists a maximal such subset J_0. We claim that $\sum_{j \in J_0} B_j = A$. It suffices to show that for all i,

$$B_i \leq \sum_{j \in J_0} B_i.$$

Well, if not, then

$$B_i \cap \left(\sum_{j \in J_0} \right) \lneq B_i,$$

and hence it is equal to zero, since B_i is simple. $\square$

(ii) $\implies$ (iii): Assume A is the direct sum $A = \sum_{i \in I} B_i$. Let

$$0 \neq a \in A, \quad a = b_{i_1} + \cdots + b_{i_k}, \quad 0 \neq b_{ij} \in B_{ij}.$$

If $Ra = 0$, then $Rb_{ij} = 0$ for all i, j. But, B_{ij} is simple, so $B_{ij} = Rb_{ij}$. Since M is simple, we pick $0 \neq b \in M$ and we see that $X := \{N \leq M \mid RN = 0\} = 0$. So if $b \neq 0$ then $b \notin X$ hence $Rb \neq 0$. Therefore, $Ra \neq 0$. Let B be a nonzero submodule of A. Then, for $i \in I$, either $B_i \subset B$ or $B_i \cap B = 0$, since B_i is simple. If $A = B$, then we're done. So, assume that there exists i such that $B_i \cap B = 0$. By **Zorn's Lemma**, there exists a maximal subset J with the property that

$$B \cap \left(\sum_{j \in J} B_i \right) = 0.$$

In that case, $\sum_{J_0 \cup \{i\}} B_j$ is direct, which contradicts the maximality of J_0.

We now claim that

$$A = B \oplus \left(\sum_{j \in J} B_j \right).$$

It suffices to show that

$$B_i \subseteq B \oplus \left(\sum_{j \in J} B_j \right)$$

for all $i \in I$. We can assume that $i \notin J$ and assume toward a contradiction that

$$B_i \not\subseteq B \oplus \left(\sum_{j \in J} B_j \right).$$

Then,

$$B \cap \left(\sum_{J \cup \{i\}} B_j \right) = 0$$

and so $B_i \cap B = 0$, i.e., $B_i \cap \sum_{j \in J} B_j = 0$. We can now write

$$b = b_i + \sum b_j$$
$$b_i = -b + \sum b_j$$
$$B_i \cap \left(B + \sum B_j \right) \neq 0.$$

This is a contradiction, which proves the claim. □

(iii) $\Longrightarrow$ (i): Let N be a submodule of A and let K be a submodule of N. By hypothesis, we can write $A = K \oplus L$ and so

$$N = N \cap A = N \cap (K \oplus L) = K \oplus (N \cap L).$$

So, K is a direct summand of N. We next show that A has simple submodules. Let $a \neq 0$ be an element of A. By **Zorn's Lemma** there exists a submodule B of A which is maximal with respect to $a \notin B$. By hypothesis, $A = B \oplus C$ for some $C \neq 0$. Also, $RC \neq 0$ by hypothesis.

We now claim that C is simple. If not, then there exists a proper nonzero submodule $D \leq C$. Then, $C = D \oplus E$ for some nonzero E. So, $A = B \oplus D \oplus E$. Then, $B < B \oplus D$ and $B < B \oplus E$.

Thus, for

$$a \in (B \oplus D) \cap (B \oplus E)$$

we have that

$$a = b + d = b' + e$$

and so

$$0 = (a - a) = (b - b') + d - e$$

which implies that $d - e = 0$ and $b = b'$, and so $a \in B$, which is a contradiction.

Now let A_0 be the sum of all simple submodules of A. Then, there exists N such that $A = A_0 \oplus N$. If $n \neq 0$, then by the preceding argument applied again, we can prove that N has a simple submodule T and so $T \subseteq A_0$ which implies that $T \subseteq A_0 \cap N = 0$, a contradiction. □

Theorem IX.3.7: The following are equivalent conditions on a ring R with 1.

(i) R is semisimple left Artinian.

(ii) Every left R-module is projective.

(iii) Every left R-module is injective.

(iv) Every short exact sequence of R-modules splits.

(v) Every nonzero unitary left R-module is semisimple.

(vi) R is a unitary semisimple left R-module.

(vii) Every left ideal is of the form Re, where e is idempotent.

(viii) R is the direct sum of minimal left ideals K_i for $i = 1, 2, \ldots, m$, such that $K_i = Re_i$ for e_i idempotent with $e_i e_j = \delta_{ij}$ and $e_1 + \cdots + e_m = 1$.

Proof: See Hungerford.

Remark: Note that in decomposing ${}_RR = \oplus Rf_i$ with f_i idempotents and R a minimal left ideal and $f_i f_j = \delta_{ij}$ and $\sum f_i = 1$, the f_i *are not* uniquely determined. This is a major source of confusion in most textbooks.

Example: Let $R = \mathrm{Mat}_n(D)$, we can let f_i be the matrices which have a 1 in the i, i spot and 0s elsewhere, *or* we can consider the set of idempotents $g_i := u f_i u^{-1}$ for any invertible $u \in R^\times$.

1.8.4 Section IX.5 - Algebras

Definition: Let K be a commutative ring with 1. Then, R is a K-algebra if $(R,+)$ is a unitary (left) K-module and $k(ab) = (ka)b = a(kb)$ for all $k \in K$ and $a, b \in R$.

Remark: If R has a 1 and K is a field, then $K1_R$ is an isomorphic copy of K in the center of R.

Remark: The ideals in an algebra, called algebra ideals must be ideals as a ring and ideals as a module. If the underlying ring has a 1, the algebra ideals coincide with the ring ideals.

Theorem IX.5.4: A semisimple left Artinian K-algebra (with K a field, so with a 1) is isomorphic to a product

$$\mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$$

where D_i are division algebras.

Definition: Let A be an algebra over a field K. An element $a \in A$ is algebraic over K if there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(a) = 0$.

Remark: Note that if A is finite dimensional as a vector space over K, then every element is algebraic.

Lemma IX.5.6: If D is an algebraic division algebra over an algebraically closed field K, then $D = K$.

Proof: D contains a copy of K in its center. If $d \in D$, then $K(d)$ is an algebraic extension field of K, hence $d \in K$. $\square$

Theorem: IX.5.7 If A is a finite dimensional semisimple algebra over an algebraically closed field K, then

$$A \cong \mathrm{Mat}_{n_1}(K) \times \cdots \times \mathrm{Mat}_{n_t}(K)$$

for some $n_i \in \mathbb{N}$.

Proposition IX.5.8: (Maschke's Theorem) Let KG be the group algebra of a finite group G over a field K. Assume that $|G|$ is a unit in K. Then KG is semisimple.

Proof: We show that every module is projective by showing that every short exact sequence of KG-modules

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{\pi} C \longrightarrow 0$$

splits. Considered as a vector space, the sequence splits. So, there exists a K-linear map

$$\theta : C \to B$$

such that

$$\pi \circ \theta = 1_C.$$

We want to make a KG-module homomorphism from θ.

Let $\psi : C \to B$ be defined by

$$\psi(c) := |G|^{-1} \sum_{g \in G} g\theta(g^{-1}c).$$

We claim that ψ is a KG-module homomorphism. For starters, ψ is a K-linear map since it's the sum of a composition of K-linear maps. Now,

$$\begin{aligned}(\pi \circ \psi)(c) &= |G|^{-1} \sum_{g \in G} \pi(g\theta(g^{-1}c)) \\ &= |G|^{-1} \sum_{g \in G} g(\pi\theta(g^{-1}c)) \\ &= |G|^{-1} \sum_{g \in G} g(g^{-1}c) \\ &= |G|^{-1} \sum_{g \in G} c \\ &= |G|^{-1}(|G|c) \\ &= c.\end{aligned}$$

Finally, we show that ψ is a KG-map. It suffices to show that for $h \in G$ and $c \in C$

$$\psi(hc) = h\psi(c).$$

Well, note that as g runs over G, so does $x := h^{-1}g$, and so

$$\begin{aligned}\psi(hc) &= |G|^{-1} \sum_{g \in G} g\theta(\underbrace{g^{-1}(hc)}_{=(g^{-1}h)c}) \\ &= |G|^{-1} \sum_{x \in G} (hx)\theta(x^{-1}c) \\ &= h\left(|G|^{-1} \sum_{x \in G} x\theta(x^{-1}c)\right) = h\psi(c).\end{aligned}$$

Hence, we've shown that every short exact sequence of KG-modules splits, i.e., every module is projective, i.e., KG is semisimple. $\square$

1.8.5 Section IX.6 - Division Algebras

Definition: An algebra A with a 1 over a field K is a central simple K-algebra if A is a simple K-algebra and the center of A is precisely K.

Example: Consider $\mathrm{Mat}_n(K)$, or $\mathbb{H}$ (the Hamilton Quaternions). Both are central simple R-algebras.

Remark: A division ring D is a central simple K-algebra, where K is defined to be the center of D.

Theorem IX.6.2: If A is a central simple K-algebra and B is a simple K-algebra, then $A \otimes_K B$ is a simple K-algebra.

Proof: Suppose that U is a nonzero ideal of $A \otimes_K B$ and let $0 \neq u \in U$. Let $\{y_i\}_{i \in I}$ be a basis of B. We write u uniquely as

$$u = \sum_{i=1}^{n} a_i \otimes y_i$$

where $0 \neq a_i \in A$. Among all such u, we can assume u to be chosen such that n is minimized.

Since A is simple, we have that $Aa_1A = A$, and so there exist r_j, s_j such that

$$1_A = \sum_{j=1}^{t} r_j a_1 s_j.$$

Now,

$$\begin{aligned} v &:= \sum_{j=1}^{t} (r_j \otimes 1) u (s_j \otimes 1) \\ &= \sum_{j=1}^{t} (r_j \otimes 1) \left[(a_1 \otimes y_1) + \sum_{i=2}^{n} a_i \otimes y_i \right] (s_j \otimes 1) \\ &= \sum_{j=1}^{t} r_j a_1 s_j \otimes y_1 + \sum_{i=2}^{n} \left[\left[\sum_{j=1}^{t} r_j a_i s_k \right] \otimes y_i \right] \\ &= 1 \otimes y_1 + \sum_{i=2}^{m} \overline{a_i} \otimes y_i \in U, \end{aligned}$$

with $\overline{a_i} \neq 0$ by minimality of n. Note that we have $v \in U$ above because U is an ideal.

Now let $a \in A$ and $w \in U$ with

$$\begin{aligned} w &:= (a \otimes 1)v - v(a \otimes 1) \\ &= \left[a \otimes y_1 + \sum a\overline{a_i} \otimes y_i \right] - \left[a \otimes y_1 + \sum \overline{a_i} a \otimes y_i \right] \\ &= \sum_{i=2}^{n} (a\overline{a_i} - \overline{a_i} a) \otimes y_i. \end{aligned}$$

By minimality, all $a\overline{a_i} - \overline{a_i} a = 0$.

Since $a \in A$ was arbitrary, we have that $\overline{a_i} \in Z(A) = K$, and therefore,

$$\begin{aligned} v &= 1 \otimes y_1 + \sum_{i=2}^{n} \overline{a_i} \otimes y_i \\ &= 1 \otimes y_1 + \sum_{i=2}^{n} 1 \otimes \overline{a_i} y_i \\ &= 1 \otimes b \end{aligned}$$

for some $b \in B$. Since B is simple, we have that $BbB = B$. Hence, there exists $c_k, d_k \in B$ such that

$$1_B = \sum_{k=1}^{m} c_k b d_k.$$

Therefore,

$$\sum_{k=1}^{m} (1 \otimes c_k)(1 \otimes b)(1 \otimes d_k) = 1 \otimes 1.$$

Since the element on the left is in U, we conclude that $1 \in U$, i.e., $U = A \otimes_K B$. Therefore $A \otimes_K B$ is simple. □

Remark: If B is actually central simple in the above proof, then this theorem can be strengthened to show that $A \otimes_K B$ is also central simple.

Theorem IX.6.3: Let D be a division ring with center K. Let F be a maximal subfield. Then, $D \otimes_K F$ is isomorphic to a dense K-subalgebra of $\mathrm{End}_F(D)$ (F acting by right multiplication).

Proof: For $x \in D$, let $\alpha_x \in \mathrm{End}_F(D)$ be defined by $\alpha_x(d) := xd$ (left multiplication). For $c \in F$, let $\beta_c \in \mathrm{End}(D)$ be defined by $\beta_c(d) = dc$ (right multiplication).

Check that $\alpha_x, \beta_c \in \mathrm{End}_F(D)$ for all $x \in D$ and $c \in F$. Also, $\alpha_x \beta_c = \beta_c \alpha_x$ for all $c \in F$ and $x \in D$. So, we get a K-bilinear map $D \times F \to \mathrm{End}_F(D)$ defined by $(x, c) \mapsto \alpha_x \beta_c$. We hence get a homomorphism of K-modules $\theta : D \otimes_K F \to \mathrm{End}_F(D)$ defined by $x \otimes c \mapsto \alpha_x \beta_c$. It needs to be checked that this is a homomorphism of algebras.

Since $D \otimes_K F$ is simple and θ is nonzero, we have that θ is a monomorphism.

Let $A = \mathrm{Im}(\theta)$. We have to show that A is a dense subring of $\mathrm{End}_F(D)$. Since D is a division ring, it is a simple left D-module, hence a simple left A-module.

Hence D is a simple faithful left A-module. So, by the **Density Theorem**, A is isomorphic to a dense subring of $\mathrm{End}_\Delta(D)$, where $\Delta = \mathrm{End}_A(D)$, (i.e., $\mathrm{End}_{\mathrm{End}_A(D)}(D)$). We claim that $\Delta = \{\beta_c \mid c \in F\}$.

It is clear that $\beta_c \in \Delta$ for all $c \in F$, since $\alpha_x \beta_c = \beta_c \alpha_x$ and F is commutative. Now let $f \in \Delta$. Then, for $x \in D$, $f(x) = f(x \cdot 1) = f(\alpha_x(1)) = \alpha_x(f(1)) = xf(1)$. Now let $c \in F$. Then, $f(c) = cf(1)$, but also $f(\beta_c(1)) = \beta_c(f(1)) = f(1) \cdot c$. Hence, $f(1) \cdot c = c \cdot f(1)$, for all $c \in F$. Therefore, by maximality of F, we have that $f(1) \in F$. Therefore, since $f(x) = xf(1)$, it follows that $f(x) = \beta_{f(1)}(x)$ for all $x \in D$, i.e., $f = \beta_{f(1)}$.

This completes the proof. □

Lemma IX.6.4: Let A be a K algebra with a 1, and let F be a field extension of K. Then, $A \otimes_K F$ is an F-algebra with a 1, and $\dim_F(A \otimes_K F) = \dim_K(A)$.

Lemma IX.6.5: Let D be a division algebra over K and let A be a finite dimensional K-algebra. Then, $D \otimes_K A$ is a left Artinian K-algebra.

Theorem IX.6.6: Let D be a division algebra with center K and let F be a maximal subfield. Then, $\dim_K(D) < \infty$ if and only if $\dim_K(F) < \infty$, in which case $\dim_F(D) = \dim_K(F)$ and $\dim_K(D) = (\dim_K(F))^2$.

Proof: Consider $D \otimes_K F$. Then,

$$\dim_F(D \otimes_K F) = \dim_K(D).$$

If $\dim_K(D) < \infty$, then $D \otimes_K F$ is a dense subring of $\mathrm{End}_F(D)$ which is finite dimensional over F, i.e., $D \otimes_K F = \mathrm{End}_F(D)$ and $\dim_F(D) < \infty$. Observe that $K \subset F \subset D$, and now, $\dim_K(F) < \infty$. The same argument shows that if $\dim_K(F) < \infty$¡ then $\dim_K(D) < \infty$.

Now note that

$$\dim_K(D) = \dim_F(D \otimes_K F) = \dim_F(\mathrm{End}_F(D)) = (\dim_F(D))^2.$$

Hence

$$\dim_K(F) \cdot \dim_F(D) = \dim_K(D) = (\dim_F(D))^2)$$

and so

$$\dim_K(F) = \dim_F(D). \ \square$$

Definition: If u is a unit of a ring R, then the ring automorphism $x \mapsto uxu^{-1}$ is called an inner automorphism.

Theorem IX.6.7: (Noether-Skolem) Let R be a simple left Artinian ring with center K. Let A, B be simple K-subalgebras of R and $\alpha : A \to B$ an isomorphism. Then, there exists $\beta \in R^\times$ such that $\alpha(a) = \beta a \beta^{-1}$, for all $a \in A$.

Proof: Think of R as $\mathrm{Hom}_D(V, V)$, where V is a finite dimensional left D-vector space and D is a division ring. Note that $K \cong Z(D)$. Now, define $\overline{A} := D \otimes_K A$ and $\overline{B} := D \otimes_K B$, so if $\alpha : A \xrightarrow{\cong} B$, then $1 \otimes \alpha : \overline{A} \xrightarrow{\cong} \overline{B}$.

V is a $D \otimes_K R$-module, since

$$(d \otimes r)(v) = d(r(v)) = r(dv).$$

Hence V is a $\overline{A} = (D \otimes_K A)$-module by restriction. This is the first $\overline{A}$-module structure on V.

Similarly, V is a $\overline{B}$-module. From this, using $\overline{\alpha}$ we get that V has a second $\overline{A}$-module structure:

$$\overline{A} \xrightarrow{1 \otimes \alpha} \overline{B}$$

defined by

$$(d \otimes a)(v) := d(\alpha(a)v) = \alpha(a)(dv).$$

Now observe that since $\overline{A}$ is a simple K-algebra, we have

(1) Every $\overline{A}$ module is semisimple.

(2) All simple $\overline{A}$ modules are isomorphic.

Since V is a finite dimensional left D-vector space, we must have (for both $\overline{A}$-module structures), that

$$V \cong^{\overline{A}} \underbrace{W \oplus \cdots \oplus W}_{t \text{ times}}$$

i.e., the two $\overline{A}$ module structures are isomorphic, i.e., there exists $\beta \in \mathrm{Hom}_K(V, V)$ and isomorphism, such that

$$(d \otimes a)(\beta(v)) = \beta((d \otimes a)(v))$$

where the multiplication on the left is in one module structure and the multiplication on the right is in the other.

So, we have that

$$d(a(\beta(v))) = \beta(d(\alpha(a)v)).$$

Set $a = 1$, and see that

$$d(\beta(v)) = \beta(d(v)).$$

Therefore, $\beta \in \mathrm{Hom}_D(V, V) = R$, i.e., $\beta \in R^\times$.

Set $d = 1$. Then,

$$a(\beta(v)) = \beta(\alpha(a)(v))$$

and therefore

$$a\beta = \beta\alpha(a)$$

in R, and hence

$$\alpha(a) = \beta^{-1}a\beta$$

for all $a \in A$. $\square$

Corollary IX.6.8: (Frobenius Theorem) If D is an algebraic division algebra over $\mathbb{R}$, then $D \cong \mathbb{R}$ or $D \cong \mathbb{C}$ or $D \cong \mathbb{H}$. Recall that

$$\mathbb{H} : +\{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ \ i^2 = j^2 = k^2 = ijk = -1\}.$$

Proof: Let K be the center of D and let F be a maximal subfield. Then,

$$R \subset K \subset F \subset D.$$

We have that K and F are algebraic over $\mathbb{R}$. Well, if $F \cong \mathbb{R}$, then $D \cong \mathbb{R}$. If $F \cong \mathbb{C}$, then if $K \cong \mathbb{C}$ we set $F = K = D \cong \mathbb{C}$. So, now assume that $F \cong \mathbb{C}$ and $K \cong \mathbb{R}$. Then, $\dim_K(F) = 2$, and so $\dim_K(D) = 4$, by **Theorem 6.6**.

We now apply the **Noether-Skolem** theorem on $A := \mathbb{C} \cong F$ and $B := F$ with $\alpha : a + ib \mapsto a - ib$, i.e., α is complex conjugation. So, there exists $\beta \in D^\times$ such that $\beta i \beta^{-1} = -i$. Then,

$$\beta^2 i \beta^{-2} = \beta(-i)\beta^{-1} = -\beta i \beta^{-1} = -(-i) = i.$$

So, β^2 commutes with i, hence with F, and therefore, $\beta^2 \in F$.

So, we can write $\beta^2 = w + iz$ for some $w, z \in \mathbb{R}$, and thus $\overline{\beta}^2 = \beta(\beta^2)\beta^{-1} = \beta^2$. Therefore, $\beta^2 \in \mathbb{R}$.

If $\beta^2 > 0$, then $\beta \in \mathbb{R}$, which is a contradiction, since $\beta \notin Z(D)$. Hence, $\beta^2 = -r^2$ for some $r > 0$. Thus,

$$\left(\frac{\beta}{r}\right)^2 = -1,$$

and so conjugation by β is the same as conjugation by $\dfrac{\beta}{r}$, so we can replace β by $\dfrac{\beta}{r}$.

Hence $D = \langle 1, i, j\rangle$ and $jij^{-1} = -i$ so $j^2 = -1$. Set $k := ij$ and check that now $D = \mathbb{H}$. $\square$

Corollary IX.6.9: (Wedderburn's Theorem) Every finite division ring is a field.

Proof: Let F be a maximal subfield of D. If $F = D$, then we're done. Hence assume $F \subsetneqq D$. Then,

$$\dim_{Z(D)}(D) = \left(\dim_{Z(D)}(F)\right)^2.$$

Let a be any element of D. Then, a lies in some maximal subfield F' and $|F'| = |F|$. Therefore, $F' \cong F$ since there is a unique finite field of any order.

Applying the Noether-Skolem theorem, there exists $\beta \in D^\times$ such that $a \in \beta F \beta^{-1}$. Thus, since a was arbitrary, we have

$$D = \bigcup_{\beta \in D^\times} \beta F \beta^{-1}.$$

Let $G := D^\times$ and let $H := F^\times$. Then,

$$G = \bigcup_{\beta \in G} \beta H \beta^{-1}.$$

But this is a contradiction to the assumption that H is proper in G and that both are finite. The reason this is a contradiction is that the number of conjugates of H is

$$\big[G : N_G(H)\big]$$

and

$$\big[G : N_G(H)\big] \leq \big[G : H\big].$$

Also,

$$\left| \bigcup_{\beta \in G} \beta H \beta^{-1} \right| \leq 1 + \big[G : H\big](|H| - 1) = |G| - (\big[G : H\big] + 1) < |G|. \ \square$$

Remark: This group theory part at the end is not a contradiction in the infinite space. Consider the group G of all rotations in space and H all rotations about a particular fixed axis. Well, if you conjugate H, you get the rotations around a different axis, and every rotation has an axis, so every rotation in G is in some conjugate of H.

1.9 Chapter X - Categories

1.9.1 Section X.1 - Functors and Natural Transformations

Remark: $\mathscr{S}$ always denotes the category of sets.

Definition: Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A covariant functor T from $\mathscr{C}$ to $\mathscr{D}$ (denoted $T : \mathscr{C} \to \mathscr{D}$) is a pair of functions: an object function and a morphism function which assigns to each morphism $C \xrightarrow{f} C'$ in $\mathscr{C}$ a morphism $T(C) \xrightarrow{T(f)} T(C')$ in $\mathscr{D}$ such that

(1) $T(1_C) = 1_{T(C)}$, for all $C \in \text{Obj}(\mathscr{C})$.

(2) $T(g \circ f) = T(g) \circ T(f)$, whenever $g \circ f$ is defined.

Definition: A contravariant functor from $\mathscr{C}$ to $\mathscr{D}$ is equivalent to a covariant functor from $\mathscr{C}$ to $\mathscr{D}^{\text{opp}}$, it reverses arrows when it maps morphisms.

Examples

(1) The identity functor $I_{\mathscr{C}} : \mathscr{C} \to \mathscr{C}$.

(2) Let R be a ring and let $\mathscr{C}$ be the category of left R-modules. For a fixed $A \in \mathscr{C}$, define $T(C) := \text{Hom}_R(A, C)$. Let f be a morphism $C \xrightarrow{f} C'$, then $T(f)$ is a map $\text{Hom}_R(A, C) \xrightarrow{T(f)} \text{Hom}_R(A, C')$, and we define $T(f)$ by $T(f) : g \mapsto f \circ g$ for all $g \in \text{Hom}_R(A, C)$. It is easy to check that this satisfies the requirements in the definition of a functor (using associativity of composition of module homomorphisms).

(3) More generally, if $\mathscr{C}$ is any category and $A \in \text{Obj}(\mathscr{C})$, define $h_A : \mathscr{C} \to \mathscr{S}$ (where $\mathscr{S}$ is the category of sets), by

$$h_A(C) = \text{hom}(A, C)$$

(where $\text{hom}(A, C)$ is the set of morphisms from A to C in $\mathscr{C}$) and for $C \xrightarrow{f} C'$, set $h_A(f) : \text{hom}(A, C) \to \text{hom}(A, C')$ by

$$h_A(f) : g \mapsto f \circ g.$$

(4) Let $\mathscr{C}$ be a concrete category. The forgetful functor is the functor $\mathscr{C} \to \mathscr{S}$ (where $\mathscr{S}$ is the category of sets), by

$$A \mapsto \text{the set } A,$$

$$f \mapsto \text{the set function } f.$$

Example: Consider the following example of a contravariant functor. Let R be a ring and let $\mathscr{C}$ be the category of left R-modules. Let A be a left R-module. We consider the contravariant Hom functor $\mathscr{C} \to \mathscr{A}$ defined by $\text{Hom}_R(-, A)$. The oject function assigns to each $C \in \text{Obj}(\mathscr{C})$ the set $\text{Hom}_R(C, A)$. For morphisms, given a morphism $C \xrightarrow{f} C'$, the map $h \mapsto h \circ f$. Once again we must check the axioms.

Example: Let R be a ring and let A be a right R-module. Then, $T_A : B \mapsto A \otimes_R B$ with, given $B \xrightarrow{f} B'$, $T(f) : A \otimes_R B \to A \otimes_R B'$ defined by $a \otimes b \mapsto a \otimes f(b)$ (which is well defined), forms a covariant functor from left R-modules to the category of abelian groups.

Remark: Composition of functors (called composite functors) works exactly as expected.

Definition: Let $T, S : \mathscr{C} \to \mathscr{D}$ be functors. A natural transformation α from T to S is a family $\{\alpha_C \mid C \in \mathscr{C}\}$ of morphisms $\alpha_c \in \hom(T(C), S(C))$, i.e.

$$T(C) \xrightarrow{\alpha_C} S(C),$$

such that for every morphism $f : C \to C'$ in $\mathscr{C}$, the diagram

$$\begin{array}{ccc} T(C) & \xrightarrow{\alpha_C} & S(C) \\ {\scriptstyle T(f)}\downarrow & & \downarrow{\scriptstyle S(f)} \\ T(C') & \xrightarrow{\alpha_{C'}} & S(C') \end{array}$$

commutes.

Example: Let R be a ring. Let $\mathscr{C}$ be the category of R-modules. Let T be the functor represented by $R \otimes_R -$, i..e, $T(B) = R \otimes_R B$. Let S be the identity functor. If f is a morphism $B \xrightarrow{f} B'$, then $T(f) : R \otimes_R B \to R \otimes_R B'$ is given by $r \otimes b \mapsto r \otimes f(b)$. For any B, define $\alpha_B : T(B) \to S(B)$ by $\alpha_B(r \otimes_R b) \mapsto rb$.

Now we check that the diagram

$$\begin{array}{ccc} R \otimes_R B & \xrightarrow{\alpha_B} & B \\ {\scriptstyle \mathrm{Id}_R \otimes f}\downarrow & & \downarrow{\scriptstyle f} \\ R \otimes_R B' & \xrightarrow{\alpha_{B'}} & B' \end{array}$$

commutes. Now, $f\alpha_B(r \otimes b) = f(rb) = rf(b)$ and $\alpha_{B'}(\mathrm{Id} \otimes f)(r \otimes b) = \alpha_{B'}(r \otimes f(b)) = rf(b)$. So, α_C is a natural transformation for all $C \in \mathscr{C}$.

Lastly, we can define $\gamma : S \to T$ and $\gamma_B : B \to R \otimes_R B$ by $b \mapsto 1 \otimes_R b$. We can check that γ is a natural transformation and that $\gamma_B \circ \alpha_B = \mathrm{Id}_B$ and $\alpha_B \circ \gamma_B = \mathrm{Id}_{R \otimes_R B}$, so α_B is an isomorphism. This gives an actual definition to the term natural isomorphism.

Example: Let X be a topological sapce. Let $\mathscr{C}$ be the category of open sets in X, where morphisms are the inclusion maps. Consider the contravariant functors from $\mathscr{C}$ to $\mathscr{S}$, where $\mathscr{S}$ is the category of sets. Then, we want to define $T : \mathscr{C} \to \mathscr{S}$ with $U \mapsto T(U)$. If $U \subset V$, then we have an inclusion map $T(V) \xrightarrow{i_{U,V}} T(U)$, e.g. $T(U) = \{\text{functions from } U \text{ to } \mathbb{R}\}$ and $T(i_{U,V})$ is the restriction map.

These functors are called presheaves on X. Let $\mathscr{P}$ be the category of presheaves on X. Then, $\mathrm{Obj}(\mathscr{P})$ are contravariant functors $T : \mathscr{C} \to \mathscr{S}$. The morphisms in this category are the natural transformations between these functors. These are called morphisms of presheaves or presheave maps.

Let S, T be presheaves. A presheave map $\alpha : S \to T$ is a family $\{\alpha_U \mid U \text{ open}\}$ with $\alpha_U : S(U) \to T(U)$ and if $U \subset V$ then we have the commutative diagram

$$\begin{array}{ccc} S(V) & \xrightarrow{\alpha_V} & T(V) \\ {\scriptstyle S(i_{U,V})}\downarrow & & \downarrow{\scriptstyle T(i_{U,V})} \\ S(U) & \xrightarrow{\alpha_U} & T(U) \end{array}$$

Definition: If $\mathscr{C}$ is a category and $A \in \mathrm{Obj}(\mathscr{C})$, then we get an automatic functor

$$h_A := \hom_{\mathscr{C}}(A, -) : \mathscr{C} \to \mathscr{S}.$$

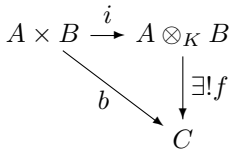
A functor $T : \mathscr{C} \to \mathscr{S}$ is representable if and only if there exists $A \in \mathrm{Obj}(\mathscr{C})$ and a natural isomorphism $\alpha : h_A \to T$. The pair (A, α) is called a representation of T.

Example: Let K be a commutative ring with 1. Let A and B be fixed K-modules. For each K-module C, let $T(C)$ be the set of K-bilinear maps $A \times B \to C$ and for $f : C \to C'$, set $T(f)(b) = f \circ b$. So given

$$A \times B \xrightarrow{b} C \xrightarrow{f} C',$$

we have $T(f) : T(C) \to T(C')$. It remains to check that T is a covariant functor from $\mathscr{M}$ (the category of K-modules) to $\mathscr{S}$.

Now we can consider the universal property of tensor products:

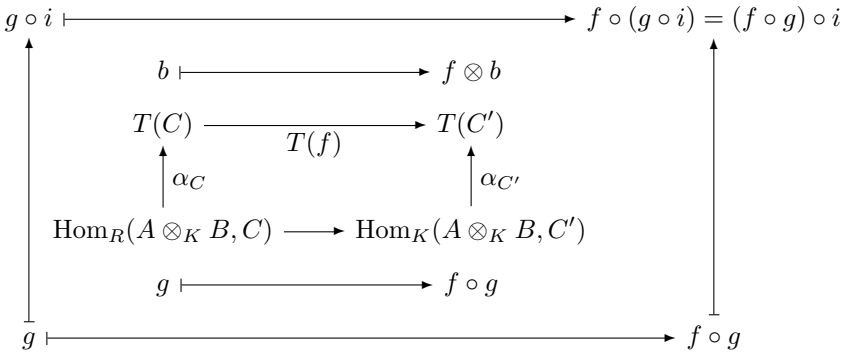


where i is given by $(a, b) \mapsto a \otimes_K b$ and f and b are K-bilinear. This we have a bijection

$$T(C) \longleftarrow \mathrm{Hom}_K(A \otimes_K B, C),$$

$$f \circ i \longleftarrow\!\shortmid f : \alpha_C.$$

It remains to check thst $\{\alpha_C\}$ gives a natural transformation. Then, T is represented by $(A \otimes_K B, \alpha)$. We have the following diagram.



Definition: Let (A, α) be a representation of $T : \mathscr{C} \to \mathscr{S}$ (note that we're implying that $A \in \mathrm{Obj}(\mathscr{C})$ and $\alpha : h_A \to T$). Let $\mathscr{C}_T$ be the category of pairs (C, s) where $C \in \mathrm{Obj}(\mathscr{C})$ and $s \in T(C)$. The morphisms from (C, s) to (D, t) in this category are the maps $f : C \to D$ such that $T(f)(s) = t$. A universal object in $\mathscr{C}_T$ is called a universal element of the functor T.

Remark: Let $(A \otimes_K B, \alpha)$ be a representative of $T : \mathscr{M} \to \mathscr{S}$ and $T(C)$ is the set of bilinear maps $A \otimes B \to C$. Then,

$$\mathscr{M}_T = \{(C, b) \mid \ C \text{ is a } K\text{-module and } b \text{ is a } K\text{-bilinear map } A \times B \to C\}.$$

Then, a morphism $(C, b) \to (C', b')$ is a map $f : C \to C'$. We showed that $(A \otimes_K B, i)$ is a universal element of T, where $i : A \times B \to A \otimes_K B$.

Lemma X.1.5: Let $T : \mathscr{C} \to \mathscr{S}$ be a covariant functor.

(i) If $\alpha : h_A \to T$ is a natural transformation and $u = \alpha_A(1_A) \in T(A)$, then for any object C of $\mathscr{C}$ and $g \in \hom_{\mathscr{C}}(A, C)$, we have $\alpha_C(g) = T(g)(u)$.

(ii) If $u \in T(A)$ and for each object C of $\mathscr{C}$ we define $\beta_C : \hom_{\mathscr{C}}(A, C) \to T(C)$ by $\beta_C(g) = T(g)(u)$, then $\beta := \{\beta_C\}_{C \in \mathrm{Obj}(\mathscr{C})}$ is a natural transformation from h_A to T such that $\beta_A(1_A) = u$.

Proof: See Hungerford.

Theorem X.1.6: Let $T : \mathscr{C} \to \mathscr{S}$ be a covariant functor. There is a one-to-one correspondence between the class X of all representations of T, and the class Y of all universal elements of T, given by

$$(A, \alpha) \mapsto (A, \alpha_A(1_A)).$$

Proof: Let (A, α) be a representation of T and set $u := \alpha_A(1_A)$. We need to show that (A, u) is actually a universal element of the category $\mathscr{C}_T$. Let $(B, s) \in \text{Obj}(\mathscr{C}_T)$. By hypothesis, we have a bijection $\alpha_B : \hom_{\mathscr{C}}(A, B) \to T(B)$. Therefore, there exists a unique $f \in \hom_{\mathscr{C}}(A, B)$ such that $\alpha_B(f) = s$. Then, $T(f)(u) = s$ (see **Lemma X.1.5(i)**). Hence, f is a morphism from (A, u) to (B, s) in $\mathscr{C}_T$. Suppose h is another morphism in $\mathscr{C}_T$ from (A, u) to (B, s). Then, $h \in \hom_{\mathscr{C}}(A, B)$ and $T(h)(u) = s$. Then, $\alpha_B(h) = T(h)(u) = s = \alpha_B(f)$. But then $h = f$ since α_B is bijective. Hence (A, u) is a universal element.

Conversely, suppose that (A, u) is a universal element of T. Then, by **Lemma X.1.5(ii)** the family

$$\beta_C : \hom_{\mathscr{C}}(A, C) \to T(C)$$

$$\beta_C(f) = T(f)(u)$$

defines a natural transformation from h_A to T. Also, $\beta_A(1_A) = u$. We want to show that (A, β) is a representation of T. It remains to show that each β_C is a bijection to conclude that β is a natural isomorphism (since we already showed that it was a natural transformation). Let $s \in T(C)$. Then, $(C, s) \in \text{Obj}(\mathscr{C}_T)$, and so there exists a unique morphism $f : A \to C$ in $\mathscr{C}$ such that $T(f)(u) = s$. But, $T(f)(u) = \beta_C(f)$ as above. Hence, β_C is surjective. Now suppose that $\beta_C(f_1) = \beta_C(f_2)$. Then, $T(f_1)(u) = T(f_2)(u) =: w$, and so f_1, f_2 are both morphisms in $\mathscr{C}_T$ taking (A, u) to (C, w). Since (A, u) is a universal object, $f_1 = f_2$, i.e., β_C in injective. Hence β_C is an isomorphism. Since C was arbitrary, we've shown that β is a natural isomorphism.

Now let $\Phi : X \to Y$ be defined by $\Phi : (A, \alpha) \mapsto (A, \alpha_A(1_A))$. Let $\Psi : Y \to X$ be defined by $\Psi : (A, u) \mapsto (A, \beta)$, where β comes from **Lemma X.1.5(ii)**. We've showed above that these two maps are well-defined (i.e., they do map to where we claim they do). We must check that $\Psi \circ \Phi = \text{Id}_X$ and that $\Phi \circ \Psi = \text{Id}_Y$. To see this, draw the commutative diagrams for all of these maps. □

Corollary X.1.7: Let $T : \mathscr{C} \to \mathscr{S}$ be a covariant functor. If (A, α) and (B, β) are representatives of T, then there exists a unique equivalence $f : A \to B$ such that for all $C \in \text{Obj}(\mathscr{C})$, the following diagram commutes.

$$\begin{array}{ccc} h_B(C) = \hom_{\mathscr{C}}(B, C) & \xrightarrow{\beta_C} & \\ \downarrow \varphi & & T(C) \\ h_A(C) = \hom_{\mathscr{C}}(A, C) & \xrightarrow{\alpha_C} & \end{array}$$

The map $\varphi : \hom_{\mathscr{C}}(B, C) \to \hom_{\mathscr{C}}(A, C)$ is given by $g \mapsto g \circ f$. We denote φ by $\hom_{\mathscr{C}}(f, 1_C)$.

Proof: Let $u = \alpha_A(1_A) \in T(A)$ and $v = \beta_B(1_B) \in T(B)$. Then, (A, u) and (B, v) are both universal objects of T, by **Theorem X.1.6**. Since these are both universal objects, there exists a unique equivalence $f : A \to B$ such that $T(f)(u) = v$. Now we much check that the diagram commutes. Consider,

$$\begin{aligned} \alpha_C(\hom_{\mathscr{C}}(f, 1_C))(g) &= \alpha_C(g \circ f) \\ &= T(g \circ f)(u) \quad \text{by applying } \textbf{Lemma X.1.5} \text{ to } \alpha \\ &= T(g)T(f)(u) \\ &= T(g)(v) \\ &= \beta_C(g) \quad \text{by applying } \textbf{Lemma X.1.5} \text{ to } \beta. \end{aligned}$$

This shows commutativity. Uniqueness of this equivalence is clear by definition. □

Corollary X.1.8: (Yoneda Lemma) Let $T : \mathscr{C} \to \mathscr{S}$ be a covariant functor. Let A be an object of $\mathscr{C}$. There is a one-to-one correspondence between the set $T(A)$ and the set $\mathrm{Nat}(h_A, T)$ of all natural transformations from h_A to T. The bijection is natural in A and T.

Proof: Define $\psi : \mathrm{Nat}(h_A, T) \to T(A)$ with $\alpha_A : h_A(A) \to T(A)$, by $\psi(\alpha) := \alpha_A(1_A)$. Define $\varphi : T(A) \to \mathrm{Nat}(h_A, T)$ by $\varphi(u) := \beta$ from **Lemma X.1.5** (where $g \in \hom_{\mathscr{C}}(A, C)$ and $\beta_C(g) := T(g)(u)$, so that $\beta_C : h_A(C) \to T(C)$ for all C (note that this family $\{\beta_C\}$ is a natural transformation)).

Now we show that φ and ψ are inverses. Firstly,

$$\begin{aligned}(\psi \circ \varphi)(u) &= \psi(\beta) \\ &= \beta_A(1_A) \\ &= T(1_A)(u) \\ &= 1_{T(A)}(u) \\ &= u.\end{aligned}$$

Next, let $u := \alpha_A(1_A)$. Then,

$$(\varphi \circ \psi)(\alpha) = \varphi(u) =: \beta.$$

So for $g \in \hom_{\mathscr{C}}(A, C)$, we have $\beta_C(g) = T(g)(u) = T(g)(\alpha_A(1_A))$. We claim that this is equal to $\alpha_C(g)$, which then shows $\alpha = \beta$, which completes the claim. To see this, consider the diagram

$$\begin{array}{ccccc} 1_A & & h & & \hom_{\mathscr{C}}(A,A) \xrightarrow{\alpha_A} T(A) \\ \downarrow & & \downarrow & & \downarrow \hom_{\mathscr{C}}(1_A, g) \qquad \downarrow T(g) \\ & & g \circ h & & \hom_{\mathscr{C}}(A,C) \xrightarrow[\alpha_C]{} T(C) \\ g & \longmapsto & & & \alpha_C(g) = T(g)(\alpha_A(1_A)) \end{array}$$

This shows that $T(g)(\alpha_A(1_A)) = \alpha_C(g)$.

We have shown the one-to-one correspondence between $T(A)$ and $\mathrm{Nat}(h_A, T)$. It remains to show that this bijection is natural in both A and T. First we show that it is natural in A. Let $f : A \to B$. We need to show that there exists a commutative diagram:

$$\begin{array}{ccc} \mathrm{Nat}(h_A, T) & \xrightarrow{\psi_A} & T(A) \\ N^*(f) \downarrow & & \downarrow T(f) \\ \mathrm{Nat}(h_B, T) & \xrightarrow{\psi_B} & T(B) \end{array}$$

where $(N^*(f)(\alpha))_C : \hom_{\mathscr{C}}(B, C) \to T(C)$ is defined by $g \mapsto \alpha_C(g \circ f)$. Note that $g \circ f \in \hom_{\mathscr{C}}(A, C)$ and so $\alpha_C(g \circ f) \in T(C)$. It must be checked that this diagram commutes.

Now we show that $\mathrm{Nat}(h_A, T)$ is natural in T. Let $\alpha : T \to S$ and consider the diagram

$$\begin{array}{ccc} \mathrm{Nat}(h_A, T) & \longrightarrow & T(A) \\ N_*(\alpha \downarrow & & \downarrow \alpha_A \\ \mathrm{Nat}(h_A, S) & \longrightarrow & S(A) \end{array}$$

We define $(N_*(\alpha))_C : \hom_{\mathscr{C}}(A, C) \to S(C)$ by $(N_*(\alpha))_C := \alpha_C \circ \beta_C$. We must check that $N_*(\alpha) = \alpha \circ \beta$ and that this diagram commutes. $\square$

Remark: Consider a functor $T : \mathscr{C} \times \mathscr{D} \to \mathscr{S}$ which is contravariant in $\mathscr{C}$ and covariant in $\mathscr{D}$. If $S : \mathscr{C} \to \mathscr{D}$ is covariant, then the map $(C, D) \mapsto \hom_{\mathscr{D}}(S(C), D)$ (which we might call the functor $\hom_{\mathscr{D}}(S(-), -)$) is an example of such a T. The next theorem asks when such a functor T will be naturally isomorphic to the

given example.

Theorem X.1.9: Let $\mathscr{C}$ and $\mathscr{D}$ be categories and T a functor $\mathscr{C} \times \mathscr{D} \to \mathscr{S}$ which is contravariant in the first variable and covariant in the second variable such that for all $C \in \text{Obj}(\mathscr{C})$ the functor $T(C, -) : \mathscr{D} \to \mathscr{S}$ is representable by (A_C, α^C) (we're just saying that A and α, depend on C, we're not actually looking at the map α_C). Then, there exists a functor $S : \mathscr{C} \to \mathscr{D}$ such that $S(C) = A_C$ for all $C \in \text{Obj}(\mathscr{C})$ and such that we have a natural isomorphism of $\hom_{\mathscr{D}}(S(-), -)$ to T. [Note that the wording of this conclusion is ambiguous in Hungerford.]

Proof: Define the object map of the functor S to be $C \mapsto A_C$. Given a morphism $C \xrightarrow{f} C'$, we need to determine $S(f)$. We have a morphism

$$\alpha^C_{A_C} : \hom_{\mathscr{D}}(A_C, A_C) \to T(C, A_C).$$

Set $u_C := \alpha^C_{A_C}(1_{A_C})$. Then, (A_C, u_C) is a universal element for $T(C, -)$. Now, we have that

$$T(f, 1_{A_C}) : T(C', A_{C'}) \to T(C, A_{C'}).$$

Let $v = T(f, 1_{A_{C'}})(u_{C'}) \in T(C, A_{C'})$. Then, by universality of (A_C, u_C), there exists a unique morphism in $\mathscr{D}$ which is

$$\overline{f} : A_C \to A_{C'}$$

such that

$$T(1_C, \overline{f})(u_C) = v.$$

This $\overline{f}$ will be our $S(f)$.

If $C \xrightarrow{\text{id}} C$ and $\overline{\text{id}} : A_C \to A_C$ maps $\overline{\text{id}} : u_C \mapsto u_C$. By the universality of (A_C, u_C), it's true that $\overline{\text{id}} = \text{id}_{A_C}$.

Now consider maps

$$C \xrightarrow{f} C' \xrightarrow{g} C''$$

We must show that $S(g \circ f) = S(g) \circ S(f)$. By construction, $S(f)$ is the unique morphism $A_{C'} \xrightarrow{\overline{g}} A_{C''}$ such that

$$T(1_{C'}, \overline{g})(u_{C'}) = T(g, 1_{A_{C''}})(u_{C''})$$

We can visualize this with the following diagram

$$\begin{array}{ccc} u_{C'} \in A_{C'} & \xrightarrow{\overline{g}} & A_{C''} \ni u_{C''} \\ \uparrow \overline{f} & & \\ u_c \in A_C & & \end{array}$$

Next, $S(f)$ is the unique morphism $A_C \to A_{C'}$ such that

$$T(1_C, \overline{f})(u_C) = T(f, 1_{A_{C'}})(u_{C'})$$

. Well, $S(g \circ f)$ must be the unique morphism $A_C \xrightarrow{\overline{h}} A_{C''}$ such that

$$T(1_C, \overline{h})(u_C) = T(g \circ f, 1_{A_{C''}})(u_{C''}).$$

Computing,

$$\begin{aligned} T(1_C, \overline{g} \circ \overline{f})(u_C) &= T(1_C, \mathbf{g}) T(1_c, \overline{f})(u_C) \\ &= T(1_C, \overline{g}) T(f, 1_{A_{C'}})(u_{C'}) \\ &= T(f, \overline{g})(u_{C'}) \\ &= T(f, 1_{A_{C''}}) T(1_C, \overline{g})(u_{C'}) \\ &= T(f, 1_{A_{C''}}) T(g, 1_{A_{C''}})(u_{C''}) \\ &= T(g \circ f, 1_{A_{C''}})(u_{C''}). \end{aligned}$$

Hence S is actually a functor.

We now consider

$$\alpha_D^C : \mathrm{Hom}_{\mathscr{D}}(S(C), D) \to T(C, D).$$

This is a functor of two variables (on the product category). In order to show naturality, we must show that for $C \xrightarrow{f} C'$ and $D \xrightarrow{g} D'$, the following diagram commutes:

$$\begin{array}{ccccc} T(C', D) & \xrightarrow{T(f,1)} & T(C, D) & \xrightarrow{T(1,g)} & T(C, D') \\ \uparrow{\scriptstyle \alpha_D^{C'}} & & \uparrow{\scriptstyle \alpha_D^{C}} & & \uparrow{\scriptstyle \alpha_{D'}^{C}} \\ \hom_{\mathscr{D}}(S(C'), D) & \longrightarrow & \hom_{\mathscr{D}}(S(C), D) & \longrightarrow & \hom_{\mathscr{D}}(S(C), D') \end{array}$$

The square on the right is commutative since

$$\alpha^C : \hom_{\mathscr{D}}(A_C, -) \to T(C, -)$$

is a natural isomorphism by assumption.

Now we must show that the left square is commutative. Let $k' \in \hom_{\mathscr{D}}(S(C'), D)$. Then,

$$\begin{aligned} T(f, 1_D)\alpha_D^{C'}(k) &= T(f, 1_D)T(1_{C'}, k)(u_{C'}) \\ &= T(1_C, k) \circ T(f, 1_{A_{C'}})(u_{C'}) \\ &= T(1_C, k)T(1_C, \overline{f})(u_C) \\ &= T(1_C, k \circ \overline{f})(u_C) \\ &= T(1_C, k \circ S(f))(u_C) \\ &= \alpha_D^C \hom_{\mathscr{D}}(S(f), 1_D)(k), \end{aligned}$$

where the last equality is by **Lemma X.1.5**. Thus commutativity is shown.

1.9.2 Section X.2 - Adjoint Functors

Unless otherwise stated, $\mathscr{S}$ is the category of sets.

Definition: Functors $S : \mathscr{C} \to \mathscr{D}$ and $T : \mathscr{D} \to \mathscr{C}$ are adjoint if there is a natural isomorphism

$$\mathrm{Hom}_{\mathscr{C}}(-, T(-)) \cong \mathrm{Hom}_{\mathscr{D}}(S(-), -).$$

Example: Let $\mathscr{C}$ be the category of sets and $\mathscr{D}$ be the category of groups. Let S be the functor which takes a set to its free group. Let T be the forgetful functor. Then, S and T are adjoint.

Example: Let R and S be rings, with A_R, ${}_RB_S$, C_S modules. Then, by an earlier theorem, there is an isomorphism

$$\mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)).$$

This isomorphism is natural in A and C. So, we have a natural isomorphism of functors

$$\mathrm{Hom}_S(- \otimes_R B,) \,\mathrm{Hom}_R(-, \mathrm{Hom}_S(B, -)).$$

Proposition X.2.2: A covariant functor $T : \mathscr{C} \to \mathscr{D}$ has a left adjoint if and only if for all $C \in \mathrm{Obj}(\mathscr{C})$, the functor

$$\hom_{\mathscr{C}}(C, T(-)) : \mathscr{D} \to \mathscr{S}$$

is representable.

Proof: Suppose that T has a left adjoint $S : \mathscr{D} \to \mathscr{C}$. Then, for all $C \in \text{Obj}(\mathscr{C})$ and $D \in \text{Obj}(\mathscr{D})$, we have

$$\hom_{\mathscr{D}}(S(C), D) \cong \hom_{\mathscr{C}}(C, T(D))$$

and this is natural in both C and D. So, we have that

$$\alpha_C^D : \hom_{\mathscr{D}}(S(C), -) \cong \hom_{\mathscr{C}}(C, T(-))$$

and $(S(C), \alpha_C)$ is a representative of $\hom_{\mathscr{C}}(C, T(-))$.

Conversely, suppose the functor $\hom_{\mathscr{C}}(C, T(-)) : \mathscr{D} \to \mathscr{S}$ is representable for each $C \in \text{Obj}(\mathscr{C})$. Then, we have an object $A_C \in \mathscr{D}$ and a natural isomorphism

$$\alpha_C : \hom_{\mathscr{D}}(A_C, -) \cong \hom_{\mathscr{C}}(C, T(-)).$$

Then, by **Theorem X.1.9**, there exists a functor $S : \mathscr{C} \to \mathscr{D}$ such that

$$S(C) = A_C$$

for all C, and we have a natural isomorphism

$$\hom_{\mathscr{D}}(S(-), -) \cong \hom_{\mathscr{C}}(-, T(-)),$$

i.e., (S, T) is an adjoint pair. □

Corollary X.2.3: A covariant functor $T : \mathscr{D} \to \mathscr{C}$ has as left adjoint if and only if for all $C \in \text{Obj}(\mathscr{C})$ there exists an object $S(C) \in \text{Obj}(\mathscr{D})$ and a morphism $u_C : \mathscr{C} \to T(S(C))$ such that $(S(C), u_C)$ is a universal element of the functor $\hom_{\mathscr{C}}(C, T(-)) : \mathscr{D} \to \mathscr{S}$.

Corollary X.2.4: Any two left adjoints of a covariant functor $T : \mathscr{D} \to \mathscr{C}$ are naturally isomorphic.

Proof: Suppose $S_1, S_2 : \mathscr{C} \to \mathscr{D}$ are left adjoints of T, with

$$\alpha : \hom_{\mathscr{D}}(S_1(-), -) \cong \hom_{\mathscr{C}}(-, T(-)),$$

$$\beta : \hom_{\mathscr{D}}(S_2(-), -) \cong \hom_{\mathscr{C}}(-, T(-)).$$

For each $C \in \text{Obj}(\mathscr{C})$, we have that $S_1(C)$ and $S_2(C)$ both represent the functor $\hom_{\mathscr{C}}(C, T(-))$. So, for each C, there is an equivalence (by **Corollary X.1.7**)

$$f_C : S_1(C) \to S_2(C)$$

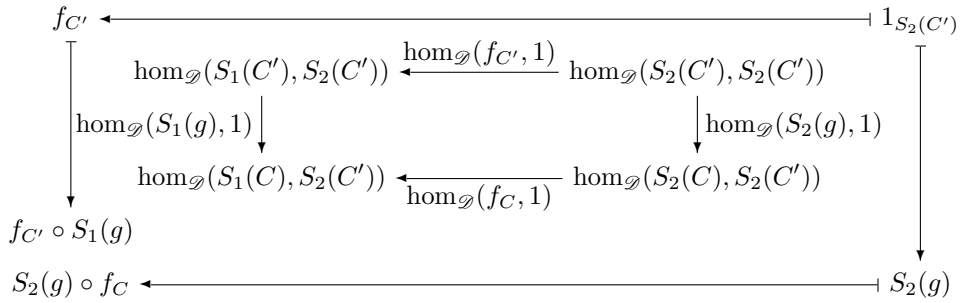
such that we have a commutative diagram for all $D \in \text{Obj}(\mathscr{D})$:

$$\begin{array}{ccc} \hom_{\mathscr{D}}(S_1(C), D) & \xrightarrow{\alpha_C} & \hom_{\mathscr{C}}(C, T(D)) \\ {\scriptstyle \hom_{\mathscr{D}}(f_C, 1)}\downarrow & \nearrow_{\beta_C} & \\ \hom_{\mathscr{D}}(S_2(C), D) & & \end{array}$$

We have to show that if $g : C \to D$ is a morphism in $\mathscr{C}$, then the following diagram commutes:

$$\begin{array}{ccc} S_1(C) & \xrightarrow{f_C} & S_2(C) \\ {\scriptstyle S_1(g)}\downarrow & & \downarrow{\scriptstyle S_2(g)} \\ S_1(C') & \xrightarrow[f_{C'}]{} & S_2(C') \end{array}$$

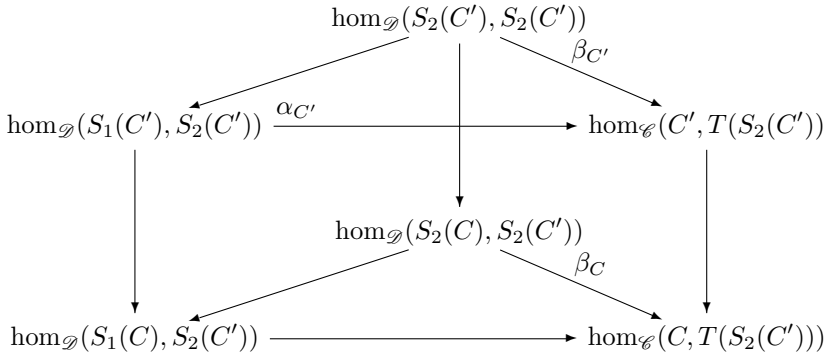
Now, in a sense, we want to hom the whole diagram, to get:



To show that this diagram commutes, we must show that

$$f_{C'} \circ S_1(g) = S_2(g) \circ f_C.$$

Then we will be done. Well, consider the redrawing in a new shape, with some additions:



Thinking of this as a triangular prism with the base facing us, the front square commutes since α is natural with respect to C, and the right square commutes by the naturality of B. It remains to see that the left square commutes. This follows from the commutativity of the top and bottom triangles, the front and right squares, and the injectivity of α_C (see Hungerford for details). □

1.9.3 Section X.3 - Morphisms

Definition: A morphism $f : C \to D$ in a category $\mathscr{C}$ is monic (or, a monomorphism) if for all $B \in \text{Obj}(\mathscr{C})$ and morphisms $g, h : B \to C$ such that $fh = fg$, we have $h = g$.

Definition: A morphism $f : C \to D$ in a category $\mathscr{C}$ is epic (or, a epimorphism) if for all $g, h : D \to E$ for some $E \in \text{Obj}(\mathscr{C})$ such that $gf = hf$, we have $g = h$.

Example: In the categories of sets, modules, groups, and abelian groups, it is true that a morphism is monic if and only if it is injective and epic if and only if it is surjective. For infinite groups, this is a bit tricky to prove.

Example: In the category of rings with identity, a ring homomorphism $f : \mathbb{Q} \to R$ is completely determined by its image on $\mathbb{Z}$. So, the inclusion map

$$\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$$

is an epimorphism, since if two functions agree on $\mathbb{Z}$, then they agree everywhere. It's clear that φ is not surjective. So, this is an example of a non-surjective epimorphism.

Example: In the category of divisible abelian groups, where morphisms are group homomorphisms, consider

$$\psi : \mathbb{Q} \xrightarrow{\nu} \mathbb{Q}/\mathbb{Z}$$

to be the natural reduction map, and consider the diagram

$$A \underset{g}{\overset{f}{\rightrightarrows}} \mathbb{Q} \xrightarrow{\nu} \mathbb{Q}/\mathbb{Z}$$

We claim that ν is a monomorphism. Suppose that $\nu \circ f = \nu \circ g$. Suppose that $f \neq g$. Then, there exists $a \in A$ such that

$$f(a) - g(a) = \frac{r}{s} \neq 0.$$

If $f(a) - g(a) \in \mathbb{Z}$ (i.e., if $s = \pm 1$), then we can pick a new s such that $\gcd(s, m) = 1$. Then there exists $b \in A$ such that $sb = a$, and so

$$s(f(b) - g(b)) = sf(b) - sg(b) = f(a) - g(a) = m,$$

i.e.,

$$f(b) - g(b) = \frac{m}{s},$$

with $s \neq \pm 1$.

Since A is divisible, there exists $b \in A$ such that $rb = a$. Then,

$$r(f(b) - f(a)) = f(a) - g(a) = \frac{r}{s} = r\left(\frac{1}{s}\right)$$

and so

$$f(b) - g(b) = \frac{1}{s}.$$

Then,

$$\nu\left(\frac{1}{s}\right) = \nu(f(b)) - \nu(g(b)) = 0$$

and so

$$\frac{1}{s} \in \mathbb{Z},$$

i.e.,

$$s = \pm 1,$$

which is a contradiction.

Definition: If $f : C \to D$ and $g : C \to D$ are morphisms, then an equalizer for (f, g) is a morphism

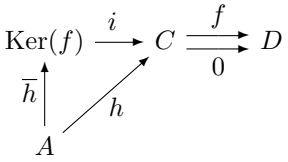
$$i : \quad B \xrightarrow{} C \underset{g}{\overset{f}{\rightrightarrows}} D$$

such that $fi = gi$ and if $h : A \to C$ satisfies $fh = gh$ then there exists a unique morphism $\overline{h} : A \to B$ such that

$$\begin{array}{ccccc} B & \xrightarrow{i} & C & \rightrightarrows & D \\ {\scriptstyle \overline{h}}\uparrow & \nearrow_{h} & & & \\ A & & & & \end{array}$$

commutes.

Example: In the case of modules, for $f : C \to D$ and $0 : C \to D$ (the zero map), we have the following diagram.



Chapter 2

Suggested Exercises

Section	Suggested Exercises
V.1	1-18
V.2	2,3,4,6,7,9,10,11,13
V.3	2,5,8,9,12,15,18,23,24
V.4	1,2,3,4,5,8,10,12,13,14
V.5	5,7,8,11
V.6	10
V.7	3,8*
V.8	10*
V.9	3*
I.7	1,(2,3,4,5),6,7
I.8	4
IV.1	4,5,6,7,9,12,16
IV.2	2
IV.3	3,5,7,8,9,10,11
IV.4	1,3,4,7,8,9
IV.5	2,3,4,5,7,8,9,10
III.4	1,3,8,10,14,15
VIII.1	1-7
VIII.2	1,6,10,15
VIII.3	3,4,6,8,9,10,11
VIII.4	1,3,4
VIII.5	1,5,7,8
VIII.6	5,7,10,11
VI.1	
VIII.7	2,3
IX.1	2,3,4,7
IX.2	1,2,4,6,11
IX.3	3,4,6,13
IX.5	4,5
X.2	3,4

Chapter 3

Summary of Facts

3.1 Chapter V - Fields And Galois Theory

3.1.1 Section V.1 - Field Extensions

Text:

- If F is an extension field of K and $u \in F$ is transcendental over K, then there is an isomorphism of fields $K(u) \cong K(x)$ which is the identity on K.
- If F is an extension field of K and $u \in F$ is algebraic, then
  (a) $K(u) = K[u]$
  (b) $K(u) \cong K[x]/(f)$ where $f \in K[x]$ is the unique irreducible monic such that $\big[f(u) = 0\big]$ and $\big[g(u) = 0$ if and only if $f \mid g\big]$.
  (c) $|K(u) : K| = n$, where $n = \deg f$ for the f described above.
  (d) $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis of the vector space $K(u)$ over K.
  (e) Every element of $K(u)$ can be written uniquely of the form $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$, for $a_i \in K$.
- Let $\sigma : K \to L$ be an isomorphism of fields. Let u be in an extension field of K and let v be in an extension field of L. If u is transcendental over K and v is transcendental over K, then σ can be extended to an isomorphism $\sigma : K(u) \to L(v)$ which maps $u \mapsto v$. On the other hand, if u is a root of an irreducible polynomial $f \in K[x]$ and v is a root of the irreducible polynomial σf, then again σ can be extended to an isomorphism $\sigma : K(u) \to L(v)$ which maps $u \mapsto v$.
- Let K be a field and let $f \in K[x]$. Let $n := \deg f$. Then, there exists a simple extension field $F = K(u)$ of K such that
  (i) $u \in F$ is a root of f,
  (ii) $\big[K(u) : K\big] \leq n$, with equality holding if and only if f is irreducible in $K[x]$,
  (iii) If f is irreducible in $K[x]$, then $K(u)$ is unique up to an isomorphism which is the identity on K.
- If F is a finite dimensional extension field of K, then F is finitely generated and algebraic over K.
- Let F be an extension of K. If $F = K(X)$ for some $X \subseteq F$ with every element of X algebraic over K, then F is an algebraic extension of K. Additionally, if $\emptyset X < \infty$, then F is finite dimensional over K.
- If F is an algebraic extension field of E and E is an algebraic extension field of K, then F is an algebraic extension of K.

- Let F be an extension of K. The set E of all elements of F that are algebraic over K is a subfield of F (which is, of course, algebraic over K). E is the unique maximal algebraic extension of K contained in F.

Exercises:

- $\big[F : K\big] = 1$ if and only if $F = K$.
- $\big[F : K\big]$ prime $\Longrightarrow$ there are no intermediate fields between F and K.
- If $u \in F$ has degree n over K, then $n \mid \big[F : K\big]$.
- A field extension can be finitely generated, but not finite dimensional. (Ex: $\mathbb{Q}(\pi) \supset \mathbb{Q}$.)
- $K(u_1, \ldots, u_n) \cong \mathrm{FOF}\big(K[u_1, \ldots, u_n]\big)$.
- For $\sigma \in S_n$, $K(u_1, \ldots, u_n) \cong K(u_{\sigma(1)}, \cdots, u_{\sigma(n)})$ and $K[u_1, \ldots, u_n] \cong K[u_{\sigma(1)}, \cdots, u_{\sigma(n)}]$.
- $K(u_1, \ldots, u_{n-1})(u_n) = K(u_1, \ldots, u_n)$ and $K[u_1, \ldots, u_{n-1}][u_n] = K[u_1, \ldots, u_n]$.
- If each u_i is algebraic over K, then $K(u_1, \ldots, u_n) = K[u_1, \ldots, u_n]$.
- Let L, M be subfields of F, and LM their composite. Then if $K \subset L \cap M$ and $M = K(S)$ for some $S \subset M$, then $LM = L(S)$.
- Every element of $K(x_1, \ldots, x_n)$ which is not in K is transcendental over K.
- If v is algebraic over $K(u)$ and v is transcendental over K, then u is algebraic over $K(v)$.
- If $\big[K(u) : K\big]$ is odd, then $K(u) = K(u^2)$.
- If F is algebraic over K and D is an integral domain such that $K \subset D \subset F$, then D is a field.
- Let L and M be intermediate fields in the extension $K \subset F$. Then

  (a) $\big[LM : K\big]$ is finite if and only if $\big[L : K\big]$ and $\big[M : K\big]$ are finite.

  (b) If $\big[MK : F\big]$ is finite, then $\big[L : K\big]$ and $\big[M : K\big]$ divide $\big[LM : K\big]$, and

  $$\big[LM : K\big] \leq \big[L : K\big]\big[M : K\big].$$

  (c) If $\big[L : K\big]$ and $\big[M : K\big]$ are finite and relatively prime, then

  $$\big[LM : K\big] = \big[L : K\big]\big[M : K\big].$$

  (d) If L and M are algebraic over K, then so is LM.
- Let L and M be intermediate fields of the extension $K \subset F$, with each having finite dimension over K. If $\big[LM : K\big] = \big[L : K\big]\big[M : K\big]$, then $L \cap M = K$. The converse holds if $\big[L : K\big]$ or $\big[M : K\big]$ equals 2.
- F is an algebraic extension of K if and only if for every intermediate field E, every monomorphism $\sigma : E \to E$ which is the identity on K is in fact an automorphism on E.
- If $u \in F$ is algebraic over $K(X)$ for some $X \subset F$, then $u \in F$ is actually algebraic over $K(X')$ for some finite $X' \subset F$.
- Let E_1, E_2 be subfields of F and let $X \subset F$. If every element of E_1 is algebraic over E_2, then every element of $E_1(X)$ is algebraic over $E_2(X)$.
- If c, d are constructible real numbers, then so are: $c + d$, $c - d$, c/d $(d \neq 0)$, cd, $\sqrt{c}$ $(c \geq 0)$. The constructible real numbers form a subfield containing (properly) $\mathbb{Q}$.

3.1.2 Section V.2 - The Fundamental Theorem

Text:

- Let F be an extension of K and let $f \in K[x]$. If $u \in F$ is a root of f and $\sigma \in \mathrm{Aut}_K F$, then $\sigma(u) \in F$ is also a root of f.
- Let F be an extension of K, with intermediate field E, and let $H \leq \mathrm{Aut}_K F$. Then

  (i) $H' := \{v \in F \mid \sigma(v) = v \text{ for all } \sigma \in H\}$ is an intermediate field of the extension.

  (ii) $E' := \{\sigma \in \mathrm{Aut}_K F \mid \sigma(u) = u \text{ for all } u \in E\} = \mathrm{Aut}_E F$ is a subgroup of $\mathrm{Aut}_K F$.
- If F is a ***finite dimensional*** Galois extension of K, then there is a bijection between the set of intermediate fields of the extension and the set of subgroups of the Galois group $\mathrm{Aut}_K F$. This bijection is given by the $'$ operator: $E \mapsto E'$ and $H \mapsto H'$. The bijection has the following properties:

  (i) The relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $\mathrm{Aut}_K F$ has order $\big[F : K\big]$.

  (ii) F is Galois over every intermediate field E, but E is Galois over K if and only if $E' \trianglelefteq G$, i.e., $\mathrm{Aut}_E F \trianglelefteq \mathrm{Aut}_K F$. In this case, $G/E' \cong \mathrm{Aut}_K E$.

  Condition (i) is not true in a non-finite dimensional Galois extension.
- If F is an extension of K, then there is a one-to-one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group,given by $E \mapsto E' = \mathrm{Aut}_E F$. The inverse of the correspondence is given by assigning to each closed subgroup H its fixed field H'.
- Let F be an extension of K, with intermediate fields L, M such that $F \supset M \supset L \supset K$. If $\big[M : L\big]$ is finite, then $\big[L' : M'\big] \leq \big[M : L\big]$. In particular, if $\big[F : K\big]$ is finite, then $\emptyset\mathrm{Aut}_K F \leq \big[F : K\big]$.
- Let F be an extension of K, and let H, J be subgroups of the Galois group $\mathrm{Aut}_K F$ with $H < K$. If $\big[J : H\big]$ is finite, then $\big[H' : J'\big] \leq \big[J : H\big]$.
- Let F be an extension of K, with intermediate fields L, M such that $F \supset M \supset L \supset K$. Let H, J be subgroups of the Galois group $\mathrm{Aut}_K F$ with $H < J$.

  (i) If L is closed and $\big[M : L\big]$ is finite, then M is closed and $\big[L' : M'\big] = \big[M : L\big]$.

  (ii) If H is closed and $\big[J : H\big]$ is finite, then J is closed and $\big[H' : J'\big] = \big[J : H\big]$.

  (iii) If F is a finite dimensional Galois extension of K, then all intermediate fields and all subgroups of the Galois group are closed and $\mathrm{Aut}_K F$ has order $\big[F : K\big]$.
- If E is a stable intermediate field of the extension F over K, then $E' = \mathrm{Aut}_E F \trianglelefteq \mathrm{Aut}_K F$.
- If $H \trianglelefteq \mathrm{Aut}_K F$, then the fixed field H' of H is a stable intermediate field of the extension.
- If F is a Galois extension field of K and E is a stable intermediate field of the extension, then E is Galois over K.
- If F is an extension of K and E is an intermediate field that is algebraic and Galois over K, then E is stable (relative to F and K).
- Let F be an extension of K with a stable intermediate field E. Then, the quotient group $\mathrm{Aut}_K F / \mathrm{Aut}_E F$ is isomorphic to the group of all K-automorphisms of E that are extendible to F.
- (Artin's Theorem) Let F be a field. Let G be a group of automorphism of F. Let K be the fixed field of G in F. Then, F is Galois over K. If G is finite, then F is a finite dimensional Galois extension of K with Galois group G.
- If G is a finite group, then there exists a Galois field extension with Galois group isomorphic to G.

Exercises:

- If $K \subsetneqq E \subseteq K(x)$, are field extensions, then $\big[K(x) : E\big]$ is finite.
- If K is an infinite field, then $K(x)$ is Galois over K. If K is finite, then $K(x)$ is not Galois over K.
- If K is an infinite field, then the only closed subgroups of $\mathrm{Aut}_K\, K(x)$ are itself and its finite subgroups.
- If E is Galois over K and F is Galois over E, and every $\sigma \in \mathrm{Aut}_K\, E$ is extendible to F, then F is Galois over K.
- If F is a finite dimensional Galois extension of K and E an intermediate field, then there exists a smallest field L such that $E \subset L \subset F$ and L is Galois over K. Furthermore,

$$\mathrm{Aut}_L\, F = \bigcap_{\sigma \in \mathrm{Aut}_K\, F} \sigma(\mathrm{Aut}_K\, F)\sigma^{-1}.$$

3.1.3 Section V.3 - Splitting Fields, Algebraic Closure, and Normality

Text:

- The splitting field of a finite set of polynomials $S := \{f_1, f_2, \ldots, f_n\}$ is equivalent to the splitting field of a single polynomial $f := f_1 f_2 \cdots f_n$.
- If K is a field and $f \in K[x]$ has degree $n \geq 1$, then there exists a splitting field F of f with $\big[F : K\big] \leq n!$.
- The following conditions on a field F are equivalent:

  (i) Every nonconstant polynomial $f \in F[x]$ has a root in F.

  (ii) Every nonconstant polynomial $f \in F[x]$ splits over F.

  (iii) Every irreducible polynomial in $F[x]$ has degree 1.

  (iv) There is no algebraic extension field of F (except F itself).

  (v) There is a field K of F such that F is algebraic over K and ever polynomial in $K[x]$ splits in $F[x]$.
- If F is an extension field of K, then the following conditions are equivalent:

  (i) F is algebraic over K and F is algebraically closed.

  (ii) F is a splitting field over K of the set of all [irreducible] polynomials in $K[x]$.
- If F is an algebraic extension field of K, then $|F| \leq \aleph_0 |K|$.
- Every field K has an algebraic closure. Any two algebraic closures of K are K-isomorphic.
- If K is a field and S a set of polynomials (of positive degree) in $K[x]$, then there exists a splitting field of S over K. (This covers the non-finite dimensional case, i.e., the splitting field of an infinite number of polynomials exists.
- Let $\sigma : K \to L$ be an isomorphism of fields. Let $S := \{f_i\}_{i \in I}$ be a set of polynomials of positive degree in $K[x]$, and let $S' = \{\sigma f_i\}_{i \in I}$ be the corresponding set of polynomials in $L[x]$. If F is a splitting field of S over K and M is a splitting field of S' over L, then σ is extendible to an isomorphism $F \cong M$.
- Let K be a field and S a set of polynomials in $K[x]$. Then any two splitting fields of S over K are K-isomorphic. In particular, any two algebraic closures of K are K-isomorphic.
- If F is an extension field of K, then the following statements are equivalent:

  (i) F is algebraic and Galois over K.

  (ii) F is separable over K and F is a splitting field over K of a set S of polynomials in $K[x]$.

  (iii) F is a splitting field over K of a set T of separable polynomials in $K[x]$.

- If F is an algebraic extension field of K, the the following statements are equivalent

  (i) F is normal over K.

  (ii) F is a splitting field over K of some set of polynomials in $K[x]$.

  (iii) If $\overline{K}$ is any algebraic closure of K containing F, then for any K-monomorphism of fields $\sigma : F \to \overline{K}$, we have that $\operatorname{Im}\sigma = F$, so that σ is actually a K-automorphism of F.

- Let F be an algebraic extension field of K. Then F is Galois over K if and only if F is normal and separable over K. If $\operatorname{char} K = 0$, then F is Galois over K if and only if F is normal in K.

- If E is an algebraic extension field of K, then there exists an extension field F of E such that

  (i) F is normal over K.

  (ii) No proper subfield of F containing E is normal over K.

  (iii) If E is separable over K, then F is Galois over K.

  (iv) $\big[F : K\big]$ is finite if and only if $\big[E : K\big]$ is finite.

  The field F is uniquely determined up to an E-isomorphism.

- If F is a finite dimensional separable extension of an infinite field K then $F = K(u)$ for some $u \in F$.

Exercises:

- If F is a splitting field of S on K and E is an intermediate field then F is a splitting field of S on E.
- If $f \in K[x]$ has $\deg f = n$, and F is a splitting field of f over K, then $\big[F : K\big]$ divides $n!$.
- No finite field is algebraically closed.
- F is an algebraic closure of K if and only if F is algebraic over K and for every algebraic extension E of K there exists a K-monomorphism $E \to F$.
- F is an algebraic closure of K if and only if F is algebraic over K and for every algebraic field extension E of another field K_1 and isomorphism of fields $\sigma : K_1 \to K$, σ extends to a monomorphism $E \to F$.
- If $u_1, \ldots, u_n \in F$ are separable over K, then $K(u_1, \ldots, u_n)$ is a separable extension over K.
- If F is generated by a (possibly infinite) set of separable elements over K, then F is a separable extension of K.
- Let E be an intermediate field of F over K. If $u \in F$ is separable over K, then u is separable over E. If F is separable over K, then F is separable over E and E is separable over K.
- Suppose $\big[F : K\big]$ is finite. Then, the following are equivalent:

  (i) F is Galois over K.

  (ii) F is separable over K and F is a splitting field of a polynomial $f \in K[x]$.

  (iii) F is a splitting field over K of a polynomial $f \in K[x]$ whose irreducible factors are separable.

- If L and M are intermediate fields such that L is a finite dimensional Galois extension of K, then LM is finite dimensional and Galois over M and $\operatorname{Aut}_M LM \cong \operatorname{Aut}_{L\cap M} L$.
- If F is algebraic Galois over K, then F is algebraic Galois over an intermediate field E.
- If F is Galois over E, E is Galois over K, and F is a splitting field over E of a family of polynomials in $K[x]$, then F is Galois over K.
- If an intermediate field E is normal over K, then E is stable (relative to F and K).
- Let F be normal over K and E an intermediate field. Then E is normal over K if and only if E is stable. Furthermore $\operatorname{Aut}_K F/E' \cong \operatorname{Aut}_K E$.

- If F is normal over an intermediate field E and E is normal of K, then F need not be normal over K. (Consider $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$.)
- If $\big[F : K\big] = 2$, then F is normal over K.
- An algebraic extension F of K is normal over K if and only if for every irreducible $f \in K[x]$, f factors in $F[x]$ as a product of irreducible factors all of which have the same degree.

3.1.4 Section V.4 - The Galois Group of a Polynomial

Text:

- Let K be a field and $f \in K[x]$ a polynomial with Galois group G. Then, G is isomorphic to a subgroup of S_n and if f is (irreducible) separable of degree n, then n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n.
- Let K be a field and $f \in K[x]$ an (irreducible) separable polynomial of degree 3. The Galois group of f is either S_3 or A_3. If $\operatorname{char} K \neq 2$ it is A_3 if and only if the discriminant of f is the square of an element of K.
- Let K be a field and $f \in K[x]$ an (irreducible) separable quartic with Galois group G (considered as a subgroup of S_4). Let α, β, γ be roots of the resolvant cubic of f and let $m = \big[K(\alpha, \beta, \gamma) : K\big]$. Then,

  (i) $m = 6 \iff G = S_4$;

  (ii) $m = 3 \iff G = A_4$;

  (iii) $m = 1 \iff G = V$;

  (iv) $m = 2 \iff G \cong D_4$ or $G \cong Z_4$; in this case $G \cong D_4$ if and only if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong Z_4$ otherwise.
- If p is prime and f is an irreducible polynomial of degree p over the field of rational numbers which has precisely two nonreal roots in the field of complex numbers, then the Galois group of f is (isomorphic to) S_p.

3.1.5 Section V.5 - Finite Fields

Text:

- If F is a finite field, then $\operatorname{char} F = p \neq 0$ for some prime p, and $|F| = p^n$ for some integer $n \geq 1$.
- If F is a field and G is a finite subgroup of the multiplicative group of nonzero elements of F, then G is a cyclic group. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.
- If F is a finite field, then F is a simple extension of its prime subfield Z_p; that is, $F = Z_p(u)$ for some $u \in F$.
- If F is a field of characteristic p and $r \geq 1$ is an integer, then the map $\varphi : F \to F$ given by $u \mapsto u^{p^r}$ is a Z_p-monomorphism of fields. If F is finite, then φ is a Z_p-automorphism of F.
- Let p be a prime and let $n \geq 1$ be an integer. Then, F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over Z_p.
- If p is a prime and $n \geq 1$ an integer, then there exists a field with p^n elements. Any two finite fields with the same number of elements are isomorphic.
- If K is a finite field and $n \geq 1$ an integer, then there exists an irreducible polynomial of degree n in $K[x]$.

- If F is a finite dimensional extension field of a finite field K, then F is finite and is Galois over K. The Galois group $\mathrm{Aut}_K F$ is cyclic.

Exercises:

- If $p \in \mathbb{Z}$ is prime, then $a^p = a$ for all $a \in Z_p$.
- If $|K| = p^n$, then every element of K has a unique p^{th} root.
- If $|K| = q$ and $f \in K[x]$ is irreducible, then f divides $x^{q^n} - x$ if and only if $\deg(f)$ divides n.
- If $|K| = p^r$ and $|F| = p^n$ then $r \mid n$ and $\mathrm{Aut}_K F$ is cyclic with generator φ given by $u \mapsto u^{p^r}$.
- Every element in a finite field may be written as the sum of two squares.
- If K is finite and F is an algebraic closure of K, then $\mathrm{Aut}_K F$ is abelian. Every nontrivial element of $\mathrm{Aut}_K F$ has infinite order.

3.1.6 Section V.6 - Separability

Text:

- Let F be an extension field of K. Then, $u \in F$ is both separable and purely inseparable over K if and only if $u \in K$.
- Let F be an extension field of K with $\mathrm{char}\, K = p \neq 0$. If $u \in F$ is algebraic over K, then u^{p^n} is separable over K for some $n \geq 0$.
- If F is an algebraic extension field of a field K of characteristic $p \neq 0$, then the following statements are equivalent:

  (i) F is purely inseparable over K;

  (ii) the irreducible polynomial of any $u \in F$ is of the form $x^{p^n} - a \in K[x]$;

  (iii) if $u \in F$, then $u^{p^n} \in K$ for some $n \geq 0$;

  (iv) the only elements of F which are separable over K are the elements of K itself;

  (v) F is generated over K by a set of purely inseparable elements.
- If F is a finite dimensional purely inseparable extension field of K and $\mathrm{char}\, K = p \neq 0$ then $\big[F : K\big] = p^n$ for some $n \geq 0$.
- Let F be an algebraic extension field of K, S the set of all elements of F which are separable over K, and P the set of all elements of F which are purely inseparable over K.

  (i) S is a separable extension field of K.

  (ii) F is purely inseparable over S.

  (iii) P is a purely inseparable extension field of K.

  (iv) $P \cap S = K$.

  (v) F is separable over P if and only if $F = SP$.

  (vi) If F is normal over K, then S is Galois over K, F is Galois over P, and $\mathrm{Aut}_K S \cong \mathrm{Aut}_P F = \mathrm{Aut}_K F$.
- If F is a separable extension field of E and E is a separable extension field of K, then F is separable over K.
- (Primitive Element Theorem) Let F be a finite dimensional extension field of K.

  (i) If F is separable over K, then F is a simple extension of K.

(ii) More generally, F is a simple extension of K if and only if there are only finitely many intermediate fields.

Exercises:

- If E is an intermediate field between F and K, then if F is purely inseparable over K we have that F is purely inseparable over E.
- If F is purely inseparable over an intermediate field E and E is purely inseparable over K, then F is purely inseparable over K.
- If $\operatorname{char} K = p \neq 0$ and $\big[F : K\big]$ is finite and not divisible by p, then F is separable over K.
- Let $\operatorname{char} K = p \neq 0$. Then an algebraic element $u \in F$ is separable over K if and only if $K(u) = K(u^{p^n})$ for all $n \geq 1$.
- If $f \in K[x]$ is irreducible of degree $m > 0$, and $\operatorname{char} K$ does not deivide m, then f is separable.
- The following conditions on a field K are equivalent, and a field that satisfies them is called perfect:

  (i) every irreducible polynomial in $K[x]$ is separable;

  (ii) every algebraic closure $\overline{K}$ of K is Galois over K;

  (iii) every algebraic extension field of K is separable over K;

  (iv) every $\operatorname{char} K = 0$ or [$\operatorname{char} K = p$ and $K = K^p$]
- Every finite field is perfect.
- Let F be an algebraic extension of K such that every polynomial in $K[x]$ has a root in F. Then F is an algebraic closure of K.

3.1.7 Section V.7 - Cyclic Extensions

Text:

- If F is a finite dimensional Galois extension field of K and

$$\operatorname{Aut}_K F = \{\sigma_1, \ldots, \sigma_n\}$$

then for any $u \in F$,

$$N_K^F(u) = \sigma_1(u) \cdots \sigma_n(u),$$
$$T_K^F(u) = \sigma_1(u) + \cdots + \sigma_n(u).$$

- $N_K^F(u) N_K^F(v) = N_K^F(uv)$.
- $T_K^F(u) + T_K^F(v) = T_K^F(u + v)$.
- Every set of distinct automorphisms of a field F is linearly independent.
- Let F be a cyclic extension of K of degree n, let σ be a generator of $\operatorname{Aut}_K F$ and let $u \in F$. Then

  (i) $T_K^F(u) = 0$ if and only if $u = v - \sigma(v)$ for some $v \in F$.

  (ii) (Hilbert's Theorem 90) $N_K^F(u) = 1_K$ if and only if $u = v\sigma(v)^{-1}$ for some nonzero $v \in F$.
- If K is a field of characteristic $p \neq 0$ and $x^p - x - 1 \in K[x]$, then $x^p - x - 1$ is either irreducible or splits in $K[x]$.
- Let n be a positive integer and K a field which contains a primitive n^{th} root of unity ξ.

  (i) If $d \mid n$, then $\xi^{n/d} = \eta$ is a primitive d^{th} root of unity in K.

(ii) If $d \mid n$ and u is a nonzero root of $x^d - a \in K[x]$, then $x^d - a$ has d distinct roots, namely $u, \eta u, \eta^2 u, \ldots, \eta^{n-1} u$, where $\eta \in K$ is a primitive d^{th} root of unity. Furthermore, $K(u)$ is a splitting field of $x^d - a$ over K and is Galois over K.

- Let n be a positive integer and K a field which contains a primitive n^{th} root of unity. Then the following conditions on an extension field F of K are equivalent.

  (i) F is cyclic of degree d, where $d \mid n$;

  (ii) F is a splitting field over K of a polynomial of the form $x^n - a \in K[x]$ (in which case $F = K(u)$, for any root u of $x^n - a$);

  (ii) F is a splitting field over K of an irreducible polynomial of the form $x^d - b \in K[x]$, where $d \mid n$ (in which case $F = K(v)$, for any root v of $x^d - b$).

Exercises:

- If n is an odd integer such that K contains a primitive n^{th} root of unity and $\operatorname{char} K \neq 2$, then K also contains a $2n^{\text{th}}$ root of unity.
- If F is a finite dimensional extension of $\mathbb{Q}$, then F contains only a finite number of roots of unity.

3.1.8 Section V.8 - Cyclotomic Extensions

Text:

- Let n be a positive integer, K a field such that $\operatorname{char} K$ does not divide n and F a cyclotomic extension of K of order n.

  (i) $F = K(\xi)$, where $\xi \in F$ is a primitive n^{th} root of unity.

  (ii) F is an abelian extension of dimension d, where $d \mid \varphi(n)$, (where φ is the Euler function); if n is prime, F is actually a cyclic extension.

  (iii) $\operatorname{Aut}_K F$ is isomorphic to a subgroup of order d of the multiplicative group of units of Z_n.

  Recall that an abelian extension is an algebraic Galois extension whose Galois group is abelian. The dimension of F over K may strictly less than $\varphi(n)$. For example, if ξ is a primitive 5^{th} root of unity in $\mathbb{C}$, then $\mathbb{R} \subset \mathbb{R}(\xi) \subset \mathbb{C}$, whence, $\big[R(\xi) : R\big] = 2 < 4 = \varphi(5)$.

3.1.9 Section V.9 - Radical Extensions

None.

3.2 Chapter I - Groups

3.2.1 Section I.7 - Categories: Products, Coproducts, and Free Objects

Text:

- Any two products of the same family of objects and maps are equivalent. The same applies to coproducts.
- If F is a free object on the set X and F' is a free object on the set X' and $|X| = |X'|$, then F and F' are equivalent.
- Any two universal [resp. couniversal] objects in a category are equivalent.

Exercises:

- If $f : A \to B$ is an equivalence in a category and $g : B \to A$ is the morphism such that $g \circ f = 1_A$ and $f \circ g = 1_B$, then g is unique.
- The product in the category of groups is the usual direct product.
- The product in the category of abelian groups is the usual direct product.
- The coproduct in the category of sets is the disjoint union.

3.2.2 Section I.8 - Direct Products and Direct Sums

Text:

- The coproduct in the category of abelian groups is the weak direct product. This is not the coproduct in the category of all groups.

Exercises:

- S_3 is not the direct product of any family of its proper subgroups. The same is true of Z_{p^n} and $\mathbb{Z}$.

3.2.3 Section I.9 - Free Groups, Free Products, Generators, and Relations

Text:

- Free objects in the category of all groups are the free groups.
- Every group is the homomorphic image of some free group.
- The coproduct in the category of all groups is the free product.

Exercises:

- Every nonidentity element in a free group F has infinite order.
- The free group on one element is isomorphic to $\mathbb{Z}$.
- A free group is a free product of infinite cyclic groups.

3.3 Chapter IV - Modules

3.3.1 Section IV.1 - Modules, Homomorphisms, and Exact Sequences

Text:

- Every additive abelian group G is a unitary $\mathbb{Z}$-module.
- If S is a ring and R is a subring, then S is an R-module. In particular, $R[x_1, \ldots, x_n]$ and $R[[x]]$ are R-modules.
- If I is a left ideal of R, then I is a left R-module.
- R/I is an R-module.
- The intersection of an arbitrary set of submodules is a submodule.
- The direct product and direct sum of R-modules are themselves R-modules.
- (The Short Five Lemma) Let R be a ring and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow[f']{} & B' & \xrightarrow[g']{} & C' & \longrightarrow & 0 \end{array}$$

  a commutative diagram of R-modules and R-module homomorphisms such that each row is a short exact sequence. Then,

  (i) α, γ monomorphisms $\Longrightarrow \beta$ is a monomorphism;

  (ii) α, γ e $\Longrightarrow \beta$ is an epimorphism;

  (iii) α, γ isomorphisms $\Longrightarrow \beta$ is an isomorphism.

- Let R be a ring and

$$0 \longrightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \longrightarrow 0$$

  be a short exact sequence of R-module homomorphisms. Then the following conditions are equivalent.

  (i) There is an R-module homomorphism $h : A_2 \to B$ with $gh = 1_{A_2}$;

  (ii) There is an R-module homomorphism $k : B \to A_1$ with $kf = 1_{A_1}$;

  (iii) The given seqience is isomorphism (with identity maps on A_1 and A_2) to the direct sum short exact sequence

$$0 \longrightarrow A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\iota_2} A_2 \longrightarrow 0$$

  In particular, $B \cong A_1 \oplus A_2$.

  A short exact sequence that satisfies these equivalent conditions is said to be split exact.

Exercises:

- Let R be a ring and R^{op} its opposite ring. If A is a left [resp. right] R-module, then A is a right [resp. left] R^{op}-module such that $ra = ar$ for all $a \in A$, $r \in R$ and $r \in R^{\text{op}}$.

3.3.2 Section IV.2 - Free Modules and Vector Spaces

Text:

- Let R be a ring with identity. The following conditions on a unitary R-module F are equivalent, and if F satisfies them it is called a free R-module.

  (i) F has a nonempty base;

  (ii) F is the internal direct sum of a family of cyclic R-modules, each of which is isomorphic as a left R-module to R;

  (iii) F is R-module isomorphic to a direct sum of copies of the left R-module R;

  (iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: given any unitary R-module A and function $f : X \to A$, there exists a unique R-module homomorphism $\overline{f} : F \to A$ such that $\overline{f} \circ \iota = f$. In other words, F is a free object in the category of unitary R-modules.

- In the category of all modules over an arbitrary but fixed ring (possibly without identity), the free objects are free modules.

- Every (unitary) module A over a ring R (with identity) is the homomorphic image of a free R-module F. If A is finitely generated, then F may be chosen to be finitely generated.

- Every vector space V over a division ring D has a basis and is therefore a free D-module. More generally, every linearly independent subset of V is contained in a basis. Additionally, every spanning subset of V contains a basis.

- Every basis of a free R-module has the same cardinality if R is a commutative ring with identity. Every basis of a vector space over a division ring has the same cardinality. This is not true for free modules over an arbitrary ring with identity.

Exercises:

- A ring R with identity, when considered as an R-module over itself, is not a free object in the category of all R-modules.

3.3.3 Section IV.3 - Projective and Injective Modules

Text:

- Every free module F over a ring R with identity is projective.
- Every module A over a ring R is the homomorphic image of a projective R-module.
- Let R be a ring. The following conditions on an R-module P are equivalent.

  (i) P is projective;

  (ii) Every short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$ is split exact (hence $B \cong A \oplus P$);

  (iii) There is a free module F and an R-module K such that $F \cong K \oplus P$.
- A direct sum of R-modules $\sum P_i$ is projective if and only if each P_i is projective.
- A direct product of R-modules $\prod J_i$ is injective if and only if each J_i is injective.
- An abelian group D is divisible if and only if D is an injective (unitary) $\mathbb{Z}$-module.
- Every abelian group A may be embedded in a divisible abelian group.
- Let R be a ring. The following conditions on a unitary R-module J are equivalent.

  (i) J is injective;

  (ii) Every short exact sequence $0 \longrightarrow J \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is split exact (hence $B \cong J \oplus C$);

  (iii) J is a direct summand of any module B of which it is a submodule.

Exercises:

- The following conditions on a ring R (with identity) are equivalent:

  (a) Every (unitary) R-module is projective.

  (b) Every short exact sequence of (unitary) R-modules is split exact.

  (c) Every (unitary) R-module is injective.
- Every vector space over a division ring D is both projective an an injective D-module.
- No nonzero finite abelian group is divisible.
- No nonzero free abelian group is divisible.
- $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module.

3.3.4 Section IV.4 - Hom and Duality

Text:

- Let R be a ring. Then $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is an exact sequence of R-modules if and only if for every R-module D

$$0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C)$$

  is an exact sequence of abelian groups.

- Let R be a ring. Then $A \xrightarrow{\theta} B \xrightarrow{\xi} C \longrightarrow 0$ is an exact sequence of R-modules if and only if for every R-module D

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\xi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\theta}} \mathrm{Hom}_R(A, D)$$

  is an exact sequence of abelian groups.

- The following conditions on modules over a ring R are equivalent.

  (i) $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is a split exact sequence of R-modules;

  (ii) $0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D;

  (iii) $0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A, D) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D;

- The following conditions on a module P over a ring R are equivalent:

  (i) P is projective;

  (ii) If $\psi : B \to C$ is an R-module epimorphism, then $\overline{\psi} : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ is an epimorphism of abelian groups.

  (iii) If $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is any short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(P, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(P, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P, C) \longrightarrow 0$$

  is an exact sequence of abelian groups.

- The following conditions on a module J over a ring R are equivalent:

  (i) J is injective;

  (ii) If $\theta : A \to B$ is an R-module monomorphisms, then $\overline{\theta} : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$ is an epimorphism of abelian groups.

  (iii) If $0 \longrightarrow A \xrightarrow{\theta} B \xrightarrow{\xi} C \longrightarrow 0$ is any short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(C, J) \xrightarrow{\overline{\xi}} \mathrm{Hom}_R(B, J) \xrightarrow{\overline{\theta}} \mathrm{Hom}_R(A, J) \longrightarrow 0$$

  is an exact sequence of abelian groups.

- Let A, B, $\{A_i \mid i \in I\}$, and $\{B_i \mid i \in I\}$ be modules over a ring R. Then there are isomorphisms of abelian groups:

  (i) $\mathrm{Hom}_R\left(\sum_{i \in I} A_i, B\right) = \prod_{i \in I} \mathrm{Hom}_R(A_i, B)$;

(ii) $\mathrm{Hom}_R\left(A, \prod_{j\in J} B_j\right) \cong \prod_{j\in J} \mathrm{Hom}_R(A, B_j)$.

- If A is a unitary left module over a ring R with identity then there is an isomorphism of left R-modules $A \cong \mathrm{Hom}_R(R, A)$.
- Let A be a left module over a ring R.

  (i) There is an R-module homomorphism $\theta : A \to A^{**}$.

  (ii) If R has an identity and A is free, then θ is a monomorphism.

  (iii) If R has an identity and A si free with a finite bases, then θ is an isomorphism.

Exercises:

- For any abelian group A and positive integer m: $\mathrm{Hom}(Z_m, A) \cong A[m] = \{a \in A \mid ma = 0\}$.
- $\mathrm{Hom}(Z_m, Z_n) \cong Z_{\gcd(m,n)}$.
- The $\mathbb{Z}$-module Z_m has $Z_m^* = 0$.
- For each $k \geq 1$, Z_m is a Z_{mk}-module; as a Z_{mk}-module, $Z_m^* \cong Z_m$.
- If R is a ring with identity, then there is a ring homomorphism

$$\mathrm{Hom}_R(R, R) \cong R^{\mathrm{op}}.$$

  In particular, if R is commutative, then

$$\mathrm{Hom}_R(R, R) \cong R.$$

- If R has an identity and we denote the left R-module R by ${}_RR$ and the right R-module R by R_R, then

$$({}_RR)^* \cong R_R \quad \text{and} \quad (R_R)^* \cong {}_RR.$$

3.3.5 Section IV.5 - Tensor Products

Text:

- If $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{} $ is an exact sequence of left modules over a ring R and D is a right R-module, then
$$D \otimes_R A \xrightarrow{1_D \otimes f} D \otimes_R B \xrightarrow{1_D \otimes g} D \otimes_R C \longrightarrow 0$$
is an exact sequence of abelian groups. An analogous statement holds for an exact sequence in the first variable.
- If R is a ring with identity and A_R and ${}_RB$ are unitary R-modules, then there are R-module isomorphisms
$$A \otimes_R R \cong A \quad \text{and} \quad R \otimes_R B \cong B.$$
- The operation of tensor product is associative.
- The operation of tensor product distributes over direct sums.

Exercises:

- Let A be an abelian group. Then for each $m > 0$: $A \otimes_{\mathbb{Z}} Z_m \cong A/mA$.
- $Z_m \otimes_{\mathbb{Z}} Z_n \cong Z_c$, where $c = \gcd(m, n)$.
- Let A be a torsion abelian group. Then: $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.
- $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$.
- Not every tensor is a simple tensor.

3.3.6 Section IV.7 - Algebras

Text:

- Every ring R is an additive abelian group, and so a $\mathbb{Z}$-module, and so a $\mathbb{Z}$-algebra.
- If K is a commutative ring with identity, then $K[x_1, \ldots, x_n]$ and $K[[x]]$ are K-algebras.
- If V is a vector space over a field F, then $\mathrm{Hom}_F(V, V)$ is an F-algebra.
- Both $\mathbb{C}$ and the ring of real quaternions are $\mathbb{R}$-division algebras.
- If K is a commutative ring with identity, then $\mathrm{Mat}_n(K)$ is a K-algebra. If A is a K-algebra, then so is $\mathrm{Mat}_n(A)$.

Exercises:

- In the category whose commutative K-algebras with identity and whose morphisms are K-algebra homomorphisms $f : A \to B$ such that $f(1_A) = 1_B$, then the coproduct of A and B is $A \otimes_K B$.
- If A and B are unitary K-modules, then there is an isomorphism of K-modules $A \otimes_K B \cong B \otimes_K A$.
- Let A be a ring with identity. Then A is a K-algebra with identity if and only if there is a ring homomorphism of K into the center of A such that $1_K \mapsto 1_A$.
- In the category whose commutative K-algebras with identity and whose morphisms are K-algebra homomorphisms $f : A \to B$ such that $f(1_A) = 1_B$, then if X is the set $\{x_1, \ldots, x_n\}$ then $K[x_1, \ldots, x_n]$ is a free object of the set X.

3.4 Chapter III - Rings

3.4.1 Section III.4 - Rings of Quotients and Localization

Text:

- Let S be a multiplicative subset of a commutative ring R.

  (i) If I is an ideal in R, then $S^{-1}I = \{a/s \mid a \in I,\ s \in S\}$ is an ideal in $S^{-1}R$.

  (ii) If J is another ideal in R, then

$$S^{-1}(I+J) = S^{-1}I + S^{-1}J,$$

$$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J),$$

$$S^{-1}(I \cap J) = S^{-1}I \cap S^{1}J.$$

- Let S be a multiplicative subset of a commutative ring R with identity and let I be an ideal of R. Then, $S^{-1}I = S^{-1}R$ if and only if $S \cap I = \emptyset$.
- There is a one-to-one correspondence between the set of prime ideals of R which are contained in P and the set of prime ideals of R_P, given by $Q \mapsto Q_P$.
- The ideal P_P in R_P is the unique maximal ideal of R_P.
- If R is a commutative ring with identity, then the following conditions are equivalent.

  (i) R is a local ring;

  (ii) all nonunits of R are contained in some ideal $M \neq R$;

  (iii) the nonunits of R form an ideal.

Exercises:

- If R is a principal ideal domain and $S \neq 0$, then $S^{-1}R$ is also a principal ideal domain.
- $S^{-1}\operatorname{Rad}(I) = \operatorname{Rad}(S^{-1}I)$.
- A commutative ring with identity is local if and only if for all $r, s \in R$ the statement $r + s = 1_R$ implies that either r or s is a unit.
- Every nonzero homomorphic image of a local ring is local.

3.5 Chapter VI - The Structure of Fields

3.5.1 Section VI.1 - Transcendence Bases

None.

3.6 Chapter VIII - Commutative Rings and Modules

3.6.1 Section VIII.1 - Chain Conditions

Text:

- A division ring D is both Noetherian and Artinian since the only left or right ideals are D and 0.
- Every commutative principal ideal ring is Noetherian.
- The ring $\mathrm{Mat}_n(D)$ over a division ring is both Noetherian and Artinian.
- If R is a left Noetherian [resp. Artinian] ring with identity then every finitely generated left R-module A satisfies the ascending [resp. descending] chain condition on submodule. This is also true if "left" is replaced by "right".
- A module A satisfies the ascending chain condition on submodules if and only if every submodule of A is finitely generated. In particular, a commutative ring R is Noetherian if and only if every ideal of R is finitely generated. There is no analogous property for the descending chain condition.

Exercises:

- If I is a nonzero ideal in a principal ideal domain R, then the ring R/I is both Noetherian and Artinian.
- Every homomorphic image of a left Noetherian [resp. Artinian] ring is left Noetherian [resp. Artinian].
- A ring R is left Noetherian [resp. Artinian] if and only if $\mathrm{Mat}_n(R)$ is left Noetherian [reps. Artinian] for every $n \geq 1$.
- An Artinian integral domain is a field.

3.6.2 Section VIII.2 - Prime and Primary Ideals

Text:

- If R is a commutative ring with identity and P is an ideal which is maximal in the set of all ideals of R which are not finitely generated, then P is prime. In any integral domain, $\text{Rad}(0) = 0$.
- If I is an ideal in a commutative ring R, then $\text{Rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n > 0\}$.
- $\text{Rad}(\text{Rad}(I)) = \text{Rad}(I)$.
- $\text{Rad}(I_1 I_2 \cdots I_n) = \text{Rad}\left(\bigcap_{j=1}^{n} I_j\right) = \bigcap_{j=1}^{n} \text{Rad}(I_j)$.
- $\text{Rad}(I^m) = \text{Rad}(I)$.
- If Q is a primary ideal in a commutative ring R, then $\text{Rad}(Q)$ is prime.
- Let Q and P be ideals in a commutative ring R. Then Q is primary for P if and only if:

  (i) $Q \subset P \subset \text{Rad}(Q)$, and

  (ii) If $ab \in Q$ and $a \notin Q$ then $b \in P$.
- The intersection of a finite number of P-primary ideals is a P-primary ideal.

Exercises:

- In a commutative Artinian ring with identity, every prime ideal is maximal, and there are only a finite number of distinct prime ideals.
- If R has an identity, then the set of all zero divisors of R is a union of prime ideals.
- If R has an identity, then $\text{Rad}(I)$ is the intersection of all minimal prime ideals.

3.6.3 Section VIII.3 - Primary Decomposition

Text:

- Let R be a commutative ring with identity and A a primary submodule of an R-module B. Then, $Q_A := \{r \in R \mid rB \subset A\}$ is a primary ideal in R.
- If R is a commutative ring with identity and B an R-module that satisfies ACC on submodules. Then every proper submodule A has a reduced primary decomposition.

Exercises:

- Consider a commutative ring R with identity as an R-module. If Q is a primary submodule of R, then Q is a primary ideal.
- If A is a P-primary submodule of an R-module B and $rx \in A$ ($r \in R$, $x \in B$), then either $r \in P$ or $x \in A$.

3.6.4 Section VIII.4 - Noetherian Rings and Modules

Text:

- A commutative ring R with identity is Noetherian if and only if every prime ideal of R is finitely generated.
- (Krull Intersection Theorem) Let R be a commutative ring with identity, I an ideal of R and A a Noetherian R-module. If $B = \bigcap_{n=1}^{\infty} I^n A$, then $IB = B$.
- (Nakayama's Lemma) If J is an ideal in a commutative ring R with identity, then the following conditions are equivalent.

  (i) J is contained in every maximal ideal of R;

  (ii) $1_R - j$ is a unit for every $j \in J$;

  (iii) If A is a finitely generated R-module such that $JA = A$, then $A = 0$l

  (iv) If B is a submodule of a finitely generated R-module A such that $A = JA + B$, then $A = B$.
- (Corollary to Nakayama) If R is a Noetherian local ring with maximal ideal M, then $\bigcap_{i=1}^{\infty} M^n = 0$.
- If R is a local ring, then every finitely generated projective R-module is free.
- (Hilbert Basis Theorem) If R is a commutative Noetherian ring with identity, then so is $R[x_1, \ldots, x_n]$.
- If R is a commutative Noetherian ring with identity, then so is $R[[x]]$.

3.6.5 Section VIII.5 - Ring Extensions

Text:

- Let S be an extension ring of R and $s \in S$. Then the following conditions are equivalent:

  (i) s is integral over R;

  (ii) $R[s]$ is a finitely generated R-module;

  (iii) there is a subring T of S containing 1_S and $R[s]$ which is finitely generated as an R-module;

  (iv) there is an $R[s]$-submodule B of S which is finitely generated as an R-module and whose annihilator in $R[s]$ is zero.

- If S is a ring extension of R and S is finitely generated as an R-module, then S is an integral extension of R.

- If T is an integral extension ring of S and S is an integral extension ring of R, then T is an integral extension ring of R.

- (Lying-over Theorem) Let S be an integral extension ring of R and P a prime ideal of R. Then there exists a prime ideal Q in S which lies over P (that is, $Q \cap R = P$).

- (Going-up Theorem) Let S be an integral extension ring of R and P_1, P prime ideals in R such that $P_1 \subset P$. If Q_1 is a prime ideal of S lying over P_1, then there exists a prime ideal Q of S such that $Q_1 \subset Q$ and Q lies over P.

- Let S be an integral extension ring of R and let Q be a prime ideal in S which lies over a prime ideal P in$R$. Then, Q is maximal in S if and only if P is maximal in R.

Exercises:

- Let S be an integral extension ring of R and suppose R and S are integral domains. Then S is a field if and only if R is a field.

- Every unique factorization domain is integrally closed.

3.6.6 Section VIII.6 - Dedekind Domains

Text:

- If R is a Dedekind domain, then every nonzero prime ideal of R is invertible and maximal.
- Every invertible fractional ideal of an integral domain R with quotient field K is a finitely generated R-module.
- If R is Noetherian, integrally closed integral domain and R has a unique nonzero prime ideal P, then R is a discrete valuation ring.
- The following conditions on an integral domain R are equivalent.

  (i) R is a Dedekind domain.

  (ii) Every proper ideal in R is uniquely a product of a finite number of prime ideals.

  (iii) Every nonzero ideal in R is invertible.

  (iv) Every fractional ideal of R is invertible.

  (v) The set of all fractional ideals of R is a group under multiplication.

  (vi) Every ideal in R in projective.

  (vii) Every fractional ideal of R is projective.

  (viii) R is Noetherian, integrally closed, and every nonzero prime ideal is maximal.

  (ix) R is Noetherian and for every nonzero prime ideal P of R, the localization R_P of R at P is a discrete valuation ring.

Exercises:

- An invertible ideal in an integral domain that is a local ring is principal.
- A discrete valuation ring is Noetherian and integrally closed.
- If S is a multiplicative subset of a Dedekind domain R (with $1_R \in S$ and $0 \notin S$), then $S^{-1}R$ is a Dedekind domain.
- If I is a nonzero ideal in a Dedekind domain R, then R/I is an Artinian ring.
- Every proper ideal in a Dedekind domain may be generated by at most two elements.

3.6.7 Section VIII.7 - The Hilbert Nullstellensatz

Text:

- (Noether Normalization Lemma) Let R be an integral domain which is a finitely generated extension ring of a field K and let r be the transcendence degree over K of the quotient field F of R. Then there exists an algebraically independent subset $\{t_1, t_2, \ldots, t_r\}$ of R such that R is integral over $K[t_1, \ldots, t_r]$.
- (Weak Hilbert Nullstellensatz) If F is an algebraically closed extension field of a field K and I is a proper ideal of $K[x_1, \ldots, x_n]$, then the affine variety $V(I)$ defined by I in F^n is nonempty.
- (Hilbert Nullstellensatz) Let F be an algebraically closed extension field of a field K and I a proper ideal of $K[x_1, \ldots, x_n]$. Let

  $$V(I) := \{(a_1, \ldots, a_n) \in F^n \mid g(a_1, \ldots, a_n) = 0 \text{ for all } g \in I\}.$$

  Then,

  $$\text{Rad}(I) = J(V(I)) := \{f \in K[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V(I)\}.$$

  In other words, $f(a_1, \ldots, a_n) = 0$ for every zero $(a_1, \ldots, a_n)$ of I in f^n if and only if $f^m \in I$ for some $m \geq 1$.

3.7 Chapter IX - The Structure of Rings

3.7.1 Section IX.1 - Simple And Primitive Rings

Text:

- A left module A over a ring R is simple if and only if A is isomorphic to R/I for some regular maximal left ideal I.
- A simple ring R with identity is primitive.
- A commutative ring R is primitive if and only if R is a field.
- Let R be a dense ring of endomorphisms of a vector space V over a division ring D. Then R is left [resp. right] Artinian if and only if $\dim_D V$ is finite, in which case $R = \mathrm{Hom}_D(V, V)$.
- (Schur) Let A be a simple module over a ring R and let B be an R-module.

  (i) Every nonzero R-module homomorphism $f : A \to B$ is a monomorphism.

  (ii) Every nonzero R-module homomorphism $g : B \to A$ is an epimorphism.

  (iii) The endomorphism ring $D = \mathrm{Hom}_R(A, A)$ is a division ring.
- (Jacobson Density Theorem) Let R be a primitive ring and A a faithful simple R-module. Consider A as a vector space over the division ring $\mathrm{Hom}_R(A, A) = D$. Then R is isomorphic to a dense ring of endomorphisms of the D-vector space A.
- (Wedderburn-Artin) The following conditions on a left Artinian ring R are equivalent.

  (i) R is simple.

  (ii) R is primitive.

  (iii) R is isomorphic to the endomorphism ring of a nonzero finite dimensional vector space V over a division ring D.

  (iv) For some positive integer n, R is isomorphic to the ring of all $n \times n$ matrices over a division ring.

Exercises:

- If R is a dense ring of endomorphisms of a vector space V and K is a nonzero ideal of R, then K is also a dense ring of endomorphisms of V.

3.7.2 Section IX.2 - The Jacobson Radical

Text:

- If R is a ring, then there is an ideal $J(R)$ of R such that:

  (i) $J(R)$ is the intersection of all left annihilators of simple left R-modules,

  (ii) $J(R)$ is the intersection of all the regular maximal left ideals of R,

  (iii) $J(R)$ is the intersection of all the left primitive ideals of R,

  (iv) $J(R)$ is a left quasi-regular left ideal which contains every left quasi-regular left ideal of R,

  (v) Statements (i)-(iv) are also true if "left" is replaced by "right".
- If I ($\neq R$) is a regular left ideal of a ring R, then I is contained in a maximal left ideal which is regular.
- Let R be a ring and let K be the intersection of all regular maximal left ideals of R. Then K is a left quasi-regular left ideal of R.
- An ideal P of a ring R is left primitive if and only if P is the left annihilator of a simple left R-module.
- Let I be a left ideal of a ring R. If I is left quasi-regular, then I is right quasi-regular.
- Let R be a ring.

  (i) If R is primitive, then R is semisimple.

  (ii) If R is simple and semisimple, then R is primitive.

  (iii) If R is simple, then R is either a primitive semisimple or a radical ring.
- If R is a left [resp. right] Artinian ring, then the radical $J(R)$ is a nilpotent ideal. Consequently, every nil left or right ideal of R is nilpotent and $J(R)$ is the unique maximal nilpotent left (or right) ideal of R.
- If R is left [resp. right] Noetherian, then every nil left or right ideal is nilpotent.
- If R is a ring, then the quotient ring $R/J(R)$ is semisimple.
- Let R be a ring and $a \in R$.

  (i) If $-a^2$ is left quasi-regular, then so is a.

  (ii) $a \in J(R)$ if and only if Ra is a left quasi-regular left ideal idea.
- If an ideal I of a ring R is considered as a ring, then $J(I) = I \cap J(R)$.
- If R is semisimple, then so is every ideal of R.
- $J(R)$ is a radical ring.
- If $\{R_i \mid i \in\}$ is a family of rings, then

$$J\left(\prod_{i\in I} R_i\right) = \prod_{i\in I} J(R_i).$$

Exercises:

- R is a division ring if and only if every element of R except one is left quasi-regular.
- The homomorphic image of a semisimple ring need not be semisimple.

3.7.3 Section IX.3 - Semisimple Rings

Text:

- A nonzero ring R is semisimple if and only if R is isomorphic to a subdirect product of primitive rings.
- (Wedderburn-Artin) The following conditions on a ring R are equivalent.

  (i) R is a nonzero semisimple left Artinian ring.

  (ii) R is a direct product of a finite number of simple ideals each of which is isomorphic to the endomorphism ring of a finite dimensional vector space over a division ring.

  (ii) There exist division rings $D_1, \ldots, D_t$ and positive integers $n_1, \ldots, n_t$ such that R is isomorphic to the ring $\text{Mat}_{n_1}(D_1) \times \cdots \times \text{Mat}_{n_t}(D_t)$.
- A semisimple left Artinian ring has an identity.
- A semisimple ring is left Artinian if and only if it is right Artinian.
- A semisimple left Artinian ring is both left and right Noetherian.
- The following conditions on a nonzero module A over a ring R are equivalent.

  (i) A is the sum of a family of simple submodules.

  (ii) A is the (internal) direct sum of a family of simple submodules.

  (iii) For every nonzero element $a \in A$, $Ra \neq 0$; and every submodule B of A is a direct summand (that is, $A = B \oplus C$ for some submodule C).

  A module that satisfies these equivalent conditions is said to be semisimple or completely reducible.
- The following conditions on a nonzero ring R with identity are equivalent.

  (i) R is semisimple left Artinian.

  (ii) Every unitary left R-module is projective.

  (iii) Every unitary left R-module is injective.

  (iv) Every short exact sequence of unitary left R-modules is split exact.

  (v) Every nonzero unitary left R-module is semisimple.

  (vi) R is itself a unitary semisimple left R-module.

  (vii) Every left ideal of R is of the form Re with e idempotent.

  (viii) R is the (internal) direct sum (as a left R-module) of minimal left ideals $K_1, \ldots, K_m$ such that $K_i = Re_i$ ($e_i \in R$) for $i = 1, 2, \ldots, m$ and $\{e_1, \ldots, e_m\}$ is a set of orthogonal idempotents with $e_1 + \cdots + e_m = 1_R$.
- Let R be a semisimple left Artinian ring.

  (i) $R = I_1 \times \cdots \times I_n$ where each I_j is a simple ideal of R.

  (ii) If J is any simple ideal of R, then $J = I_k$ for some k.

  (iii) If $R = J_1 \times \cdots \times J_m$ with each J_k a simple ideal of R, then $n = m$ and (after reindexing) $I_k = J_k$ for $k = 1, 2, \ldots, n$.
- Let R be a semisimple left Artinian ring.

  (i) Every simple left [resp. right] R-module is isomorphic to a minima left [resp. right] ideal of R.

  (ii) The number of nonisomorphic simple left [resp. right] R-modules is the same as he number of simple components of R.

Exercises:

- A commutative semisimple left Artinian ring is a direct product of fields.
- Every nonzero homomorphic image and every nonzero submodule of a semisimple module is semisimple.
- The intersection of two semisimple submodules is 0 or semisimple.

3.7.4 Section IX.5 - Algebras

Text:

- Let A be a K-algebra.

  (i) A subset I of A is a regular maximal left algebra ideal if and only if I is a regular maximal left ideal of the ring A.

  (ii) The Jacobson radical of the ring A coincides with the Jacobson radical of the algebra A. In particular A is a semisimple ring if and only if A is a semisimple algebra.

- Let A be a K-algebra. Every simple algebra A-module is a simple module over the ring A. Every simple module M over the ring A can be given a unique K-module structuce in such a way that M is a simple algebra A-module.

- A is a semisimple left Artinian K-algebra if and only if there is an isomorphism of K-algebras

$$A \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t),$$

  where each n_i is a positive integer and each D_i a division algebra over K.

- If D is an algebraic division algebra over an algebraically closed field K, then $D = K$.

- Let A be a finite dimensional semisimple algebra over an algebraically closed field K. Then there are positive integers $n_1, \ldots, n_t$ and an isomorphism of K-algebras

$$A \cong \mathrm{Mat}_{n_1}(K) \times \cdots \mathrm{Mat}_{n_t}(K).$$

- (Maschke) Let $K(G)$ be the group algebra of a finite group G over a field K. If K has characteristic 0, then $K(G)$ is semisimple. If K has prime characteristic p, then $K(G)$ is semisimple if and only if p does not divide $|G|$.

- (Corollary of Maschke) Let $K(G)$ be the group algebra of a finite group G over an algebraically closed field K. If $\mathrm{char}\, K = 0$ or $\mathrm{char}\, K = p$ and $p \nmid |G|$, then there exist positive integers $n_1, \ldots, n_t$ and an isomorphism of K-algebras

$$K(G) \cong \mathrm{Mat}_{n_1}(K) \times \cdots \times \mathrm{Mat}_{n_t}(K).$$

Exercises:

- A finite dimensional algebra over a field K satisfies both the ascending and descending chain conditions on left and right algebra ideals.

3.7.5 Section IX.6 - Division Algebras

Text:

- If A is a central simple algebra over a field K and B is a simple K-algebra with identity, then $A \otimes_K B$ is a simple K-algebra.

3.8 Chapter X - Categories

3.8.1 Section X.1 - Functors and Natural Transformations

None

3.8.2 Section X.2 - Adjoint Functors

Text:

- A covariant functor $T : \mathscr{D} \to \mathscr{C}$ has a left adjoint if and only if for each object $C \in \mathscr{C}$ the functor $\hom_{\mathscr{C}}(C, T(-)) : \mathscr{D} \to \mathscr{S}$ is representable.
- Any two left adjoints of a covariant functor $T : \mathscr{D} \to \mathscr{C}$ are naturally isomorphic.

Exercises:

- If $T : \mathscr{C} \to \mathscr{S}$ is a covariant functor that has a left adjoint, then T is representable.

3.8.3 Section X.3 - Morphisms

None.

Chapter 4

Examples and Counterexamples

4.1 Chapter V - Fields And Galois Theory

- **A finitely generated field extension which is not finite dimensional:**
  $\mathbb{Q}(\pi)$ is finitely generated over $\mathbb{Q}$, but is not finite dimensional.
- **Two fields that are isomorphic as vector spaces, but not as fields:**
  $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$.
- **Fields $F \supsetneq K$ with $\mathrm{Aut}_K F = 1$:**
  Let u be the real cube root of 2. Then, $\mathrm{Aut}_{\mathbb{Q}} \mathbb{Q}(u) = 1$. Also, $\mathrm{Aut}_{\mathbb{Q}} \mathbb{R} = 1$.
- **A polynomial which is separable over $\mathbb{Q}$, but not separable over some other field:**
  $x^2 + 1 \in \mathbb{Q}[x]$ is separable because it factors in $\mathbb{C}[x]$ as $x^2 + 1 = (x + i)(x - i)$. Over $Z_2[x]$, $x^2 + 1$ is not separable because its not even irreducible: $x^2 + 1 = (x + 1)^2$ in $Z_2[x]$.
- **Fields $F \supset E \supset K$ such that F is normal over E and E is normal over K, but F is not normal over K:**
  Consider $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2} \supset \mathbb{Q}$. Recall that extensions of degree 2 are normal.

4.2 Chapter I - Groups

None.

4.3 Chapter IV - Modules

- **A finitely generated R-module which is not finitely generated as an abelian group:**
  $\mathbb{Q}$.
- **A submodule a free module which is not free:**
  Consider that Z_6 is a free Z_6-module, but the submodule $\{0, 2, 4\}$ is not a free Z_6-module (because it's too small).
- **An abelian group which is not divisible:**
  Any nonzero finite abelian group or nonzero free abelian group is not divisible.
- **A projective module which is not free:**
  Z_2 and Z_3 can be made into Z_6-modules. $Z_6 = Z_2 \oplus Z_3$, and since Z_6 is a free Z_6-modules, both Z_2

and Z_3 are projective Z_6-modules (as they are summands of a free Z_6-module. However, they are not free, because they are too small.

- **R-modules A_R and ${}_RB$ such that $A \otimes_R B \neq A \otimes_{\mathbb{Z}} B$:**
  Note that $\mathbb{Z}[x]$ is a $\mathbb{Z}$-module and $\mathbb{Z}$ is a $\mathbb{Z}[x]$-module (defining x to act trivially). Now, $\mathbb{Z} \otimes_{\mathbb{Z}[x]} \mathbb{Z}[x] \otimes \mathbb{Z}$ and $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}[x] \otimes \mathbb{Z}[x]$.

4.4 Chapter III - Rings

- **A finite local ring:**
  Z_{p^n} has unique maximal ideal (p).

4.5 Chapter VI - The Structure of Fields

None.

4.6 Chapter VIII - Commutative Rings and Modules

- **A ring which is integrally closed in one extension, but not in a larger extension:**
  $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, but not in $\mathbb{C}$.
- **A Dedekind domain which is not a principal ideal domain:**
  $\mathbb{Z}[\sqrt{10}]$. This is nontrivial to prove.

4.7 Chapter IX - The Structure of Rings

- **An algebraic algebra:**
  If A is finite dimensional, then A is an algebraic algebra. For if $\dim_K A = n$ and $a \in A$, then the $n+1$ elements $a, a^2, a^3, \ldots, a^{n+1}$ must be linearly dependent. Thus, $f(a) := k_1 a + k_2 a^2 + \cdots + k_{n+1} a^{n+1} = 0$ for some $k_i \in K$ not all zero,. Thus $f(a) = 0$.
- **An infinite dimensional simple algebraic algebra:**
  The algebra of countable infinite matrices over a field K with only a finite number of nonzero entries.
- **A $\mathbb{Q}$-algebra which is a left Artinian $\mathbb{Q}$-algebra but which is not a left Artinian ring:**
  Let A be a one-dimensional vector space over the rational field. Define $ab = 0$ for all $a, b \in A$.

4.8 Chapter X - Categories

None.

Chapter 5

Study Quizzes

5.1 Chapter V - Fields And Galois Theory

1. Define an algebraic element. Define a transcendental element.
2. Define an algebraic extension. Define a transcendental extension.
3. (Theorem V.1.5) Let F be an extension field of K and $u \in F$ transcendental over K. Prove that there is an isomorphisms of fields $K(u) \cong K(x)$ which is the identity on K.
4. (Theorem V.2.2) Let F be an extension field of K and $f \in K[x]$. If $u \in F$ is a root of F and $\sigma \in \mathrm{Aut}_K F$, then $\sigma(u) \in F$ is also a root of f.
5. Define the fixed field of a subgroup. Define the subgroup corresponding to an intermediate field.
6. Define a Galois extension.
7. (Theorem V.2.5) State the Fundamental Theorem of Galois Theory.
8. Define the splitting field of a polynomial.
9. Define a separable element. Define a separable polynomial. Define a separable extension.
10. Define a normal extension. Define a normal closure.
11. Define the Galois group of a polynomial.
12. (Theorem V.4.11) Fill in the blanks. Let K be a field and $f \in K[x]$ an (irreducible) separable quartic with Galois group G (considered as a subgroup of S_4). Let α, β, γ be roots of the resolvant cubic of f and let $m = \big[K(\alpha, \beta, \gamma) : K\big]$. Then,

    (i) $m = \_\_ \iff G = \_\_$;

    (ii) $m = \_\_ \iff G = \_\_$;

    (iii) $m = \_\_ \iff G = \_\_$;

    (iv) $m = \_\_ \iff G \cong \_\_$ or $G \cong \_\_$; in this case $G \cong \_\_$ if and only if f is irreducible over $K(\alpha, \beta, \gamma)$ and $G \cong \_\_$ otherwise.
13. (Theorem V.4.12) Prove that if p is prime and f is an irreducible polynomial of degree p over the field of rational numbers which has precisely two nonreal roots in the field of complex numbers, then the Galois group of f is (isomorphic to) S_p.

14. (Proposition V.5.6 / Corollary V.5.7) Prove that is p is a prime and $n \geq 1$ is an integer, F is a finite field with p^n elements if and only if F is a splitting field of $x^{p^n} - x$ over Z_p. Prove that there exists a field with p^n elements. Prove that any two finite fields with the same number of elements are isomorphic.
15. Define a purely inseparable element, a purely inseparable polynomial, and a purely inseparable extension.
16. (Corollary V.6.8) Prove that if F is a separable extension field of E and E is separable extension field of K, then F is separable over K.
17. (Exercise V.6.2) Prove that if $u \in F$ is purely inseparable over K, then u is purely inseparable over any intermediate field E. Hence if F is purely inseparable over K, then F is purely inseparable over E.
18. (Exercise V.6.3) Prove that if F is purely inseparable over an intermediate field E and E is purely inseparable over K, then F is purely inseparable over K.
19. Define norm and trace.
20. (Theorem V.7.6(ii)) State and prove Hilbert's Theorem 90.
21. Define a cyclotomic extension.
22. Define a radical extension.

5.2 Chapter I - Groups

1. Define a category.
2. Define what it means for two objects in a category to be equivalent.
3. Define the product in a category.
4. Define the coproduct in a category.
5. (Theorem I.7.3) Prove that two products of the same family of objects with the same morphisms are equivalent.
6. (Theorem I.7.5) Prove that two coproducts of the same family of objects with the same morphisms are equivalent.
7. Define a concrete category.
8. Define a free object.
9. (Theorem I.7.8) Prove that two free objects on sets of the same cardinality are equivalent.
10. Define universal (initial) and couniversal (terminal) objects.
11. (Theorem 1.7.10) Prove that any two universal objects in a category are equivalent.
12. (Theorem 1.9.2) Prove that the free group is the free object in the category of groups.
13. (Theorem 1.9.3) Prove that every group is the homomorphic image of a free group.

5.3 Chapter IV - Modules

1. Define a module.
2. Define a module homomorphism.
3. Define what it means for a pair of module homomorphisms to be exact.

4. Define what it means for a sequence of modules to be an exact sequence.
5. Define a split exact sequence.
6. (Theorem IV.1.17) State and prove the Short Five Lemma.
7. (Theorem IV.1.18) Let R be a ring and

$$0 \longrightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \longrightarrow 0$$

be a short exact sequence of R-module homomorphisms. Prove that the following conditions are equivalent.

(i) There is an R-module homomorphism $h : A_2 \to B$ with $gh = 1_{A_2}$;

(ii) There is an R-module homomorphism $k : B \to A_1$ with $kf = 1_{A_1}$;

(iii) The given sequence is isomorphism (with identity maps on A_1 and A_2) to the direct sum short exact sequence

$$0 \longrightarrow A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\iota_2} A_2 \longrightarrow 0$$

In particular, $B \cong A_1 \oplus A_2$.

A short exact sequence that satisfies these equivalent conditions is said to be split exact.

8. (Exercise IV.1.12) State and prove the Five Lemma.
9. Define a free module.
10. Define a projective module.
11. (Theorem IV.3.2) Prove that every free module over a ring with identity is projective.
12. (Theorem IV.3.4) Let R be a ring. The following conditions on an R-module P are equivalent.

(i) P is projective;

(ii) Every short exact sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} P \longrightarrow 0$ is split exact (hence $B \cong A \oplus P$);

(iii) There is a free module F and an R-module K such that $F \cong K \oplus P$.

13. (Theorem IV.3.5) Prove that a direct sum of R-modules $\sum P_i$ is projective if and only if each P_i is projective.
14. Define an injective module.
15. (Theorem IV.3.7) Prove that a direct product of R-modules $\prod_{i \in I} J_i$ is injective if and only if J_i is injective for every $i \in I$.
16. (Theorem IV.3.9) Prove that an abelian group D is divisible if and only if D is injective (unitary) $\mathbb{Z}$-module.
17. (Theorem IV.3.10) Prove that every abelian group A may be embedded in a divisible abelian group.
18. (Exercise IV.3.1) Prove that the following conditions on a ring R (with identity) are equivalent:

(a) Every (unitary) R-module is projective.

(b) Every short exact sequence of (unitary) R-modules is split exact.

(c) Every (unitary) R-module is injective.

19. (Theorem IV.4.2) Let R be a ring. Prove that $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C$ is an exact sequence of R-modules if and only if for every R-module D

$$0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C)$$

is an exact sequence of abelian groups.

20. (Theorem IV.4.3) Let R be a ring. Prove that $A \xrightarrow{\theta} B \xrightarrow{\xi} C \longrightarrow 0$ is an exact sequence of R-modules if and only if for every R-module D

$$0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\xi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\theta}} \mathrm{Hom}_R(A, D)$$

is an exact sequence of abelian groups.

21. (Theorem IV.4.4) Prove that the following conditions on modules over a ring R are equivalent.

    (i) $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is a split exact sequence of R-modules;

    (ii) $0 \longrightarrow \mathrm{Hom}_R(D, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(D, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(D, C) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D;

    (iii) $0 \longrightarrow \mathrm{Hom}_R(C, D) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(B, D) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(A, D) \longrightarrow 0$ is a split exact sequence of abelian groups for every R-module D;

22. (Theorem IV.4.5) Prove that the following conditions on a module P over a ring R are equivalent:

    (i) P is projective;

    (ii) If $\psi : B \to C$ is an R-module epimorphism, then $\overline{\psi} : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ is an epimorphism of abelian groups.

    (iii) If $0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$ is any short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(P, A) \xrightarrow{\overline{\varphi}} \mathrm{Hom}_R(P, B) \xrightarrow{\overline{\psi}} \mathrm{Hom}_R(P, C) \longrightarrow 0$$

    is an exact sequence of abelian groups.

23. (Theorem IV.4.6) Prove that the following conditions on a module J over a ring R are equivalent:

    (i) J is injective;

    (ii) If $\theta : A \to B$ is an R-module monomorphisms, then $\overline{\theta} : \mathrm{Hom}_R(B, J) \to \mathrm{Hom}_R(A, J)$ is an epimorphism of abelian groups.

    (iii) If $0 \longrightarrow A \xrightarrow{\theta} B \xrightarrow{\xi} C \longrightarrow 0$ is any short exact sequence of R-modules, then

$$0 \longrightarrow \mathrm{Hom}_R(C, J) \xrightarrow{\overline{\xi}} \mathrm{Hom}_R(B, J) \xrightarrow{\overline{\theta}} \mathrm{Hom}_R(A, J) \longrightarrow 0$$

    is an exact sequence of abelian groups.

24. Define a middle-linear map.

25. Define a tensor product.

26. State the Universal Property for tensor products over middle-linear maps.

27. Define a bilinear map.

28. State the Universal Property for tensor products over bilinear maps.

29. (Theorem IV.5.7) Prove that if R is a ring with identity and A_R and ${}_RB$ are unitary R-modules, then there are R-module isomorphisms $A \otimes_R R \cong A$ and $R \otimes_R B \cong B$.
30. Define a K-algebra.
31. Define a division algebra.
32. Define an algebra ideal.
33. Define a K-algebra homomorphism.

5.4 Chapter III - Rings

1. Define a multiplicative subset.
2. Define what we mean by $S^{-1}R$.
3. Define the localization of R at P.
4. Define a local ring.

5.5 Chapter VI - The Structure of Fields

1. Define algebraically dependent. Define algebraically independent.
2. Define a transcendence basis.
3. Define transcendence degree.
4. Define a purely transcendental extension.

5.6 Chapter VIII - Commutative Rings and Modules

1. Define what it means for a module A to satisfy the ascending chain condition on submodules.
2. Define what it means for a module A to satisfy the descending chain condition on submodules.
3. Define what it means for a ring to satisfy the ascending chain condition.
4. Define what it means for a ring to satisfy the descending chain condition.
5. State the maximum and minimum condition on submodules.
6. (Theorem VIII.1.5 / Corollary VIII.1.6 / Corollary VIII.1.7) Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of modules. Prove that B satisfies the ascending [resp. descending] chain condition on submodules if and only if A and C satisfy it.

Prove as a corollary that if A is a submodule of a module B, then B satisfies the ascending [resp. descending] chain condition if and only if A and B/A satisfy it.

Prove as a corollary that if $A_1, A_2, \ldots, A_n$ are modules then the direct sum $A_1 \oplus \cdots \oplus A_n$ satisfies the ascending [resp. descending] chain condition on submodules if and only if each A_i satisfies it.

7. Define the following: a normal series, factors, length, refinement, proper refinement, equivalence, composition series.

8. Define a prime ideal.
9. Define a primary ideal.
10. Define the radical of an ideal I.
11. (Theorem VIII.2.6) Prove that if I is an ideal in a commutative ring R, then $\text{Rad}(I) = \{r \in R \mid r^n \in I \text{ for some } n > 0\}$.
12. Define what it means for an ideal to be P-primary.
13. Define the primary decomposition of an ideal. Define the reduced primary decomposition of an ideal.
14. Define a primary submodule.
15. Define the primary decomposition of a module.
16. (Theorem VIII.3.6) Prove the following: Let R be a commutative ring with identity and B an R-module satisfying the ascending chain condition on submodules. Then every submodule $A(\neq B)$ has a reduced primary decomposition. In particular, every submodule $A(\neq B)$ of a finitely generated module B over a commutative Noetherian ring R and every ideal $(\neq R)$ of R has a reduced primary decomposition.
17. (Proposition VIII.4.1) Prove that a commutative ring R with identity is Noetherian if and only if every prime ideal of R is finitely generated.
18. (Theorem VIII.4.4) State and prove the Krull Intersection Theorem.
19. (Lemma VIII.4.5) State and prove Nakayama's Lemma.
20. (Theorem VIII.4.9) State and prove the Hilbert Basis Theorem.
21. (Proposition VIII.4.10) Prove that if R is a commutative Noetherian ring with identity, then so is $R[[x]]$.
22. Define an extension ring.
23. Define an integral extension.
24. (Theorem VIII.5.6) If T is an integral extension ring of S and S is an integral extension ring of R, then T is an integral extension ring of R.
25. Define an integrally closed extension.
26. (Theorem VIII.5.9) State and prove the Lying-Over Theorem.
27. (Corollary VIII.5.10) State and prove the Going-Up Theorem.
28. (Exercise VIII.5.8) Prove that every unique factorization domain is integrally closed.
29. Define a Dedekind domain.
30. Define a fractional ideal.
31. Define an invertible ideal.
32. State as many equivalent properties to "R is a Dedekind domain" as you can think of. There are 8.
33. Define a discrete valuation ring.
34. (Exercise VIII.6.5) Prove that a discrete valuation ring R is Noetherian and integrally closed.
35. (Exercise VIII.6.7) Prove that if S is a multiplicative subset of a Dedekind domain R (with $1_R \in S$, $0 \notin S$), then $S^{-1}R$ is a Dedekind domain.
36. (Exercise VIII.6.10) If I is a nonzero ideal in a Dedekind domain R, then R/I is Artinian.
37. (Exercise VIII.6.11) Every proper ideal in a Dedekind domain may be generated by at most two elements.
38. Define $V(S)$ and $J(Y)$ as in section VIII.7.

39. (Theorem VIII.7.2) State and prove the Noether Normalization Lemma.
40. (Theorem VIII.7.3) State and prove the Weak Hilbert Nullstellenatz.
41. (Theorem VIII.7.4) State and prove the Hilbert Nullstellensatz.

5.7 Chapter IX - The Structure of Rings

1. Define a simple module.
2. Define a simple ring.
3. Define a regular left ideal. Define a regular right ideal.
4. Define the left annihilator. Define the right annihilator.
5. Define a faithful left module. Define a faithful right module.
6. Define a left primitive ring. Define a right primitive ring.
7. (Proposition IX.1.6) Prove that a simple ring R with identity is primitive.
8. (Proposition IX.1.7) Prove that a commutative ring R is primitive if and only if R is a field.
9. Define a dense ring of endomorphism.
10. (Theorem IX.1.12) State and prove that Jacobson Density Theorem.
11. (Theorem IX.1.14) State the Wedderburn-Artin theorem about equivalences on a left Artinian ring R (there are four equivalences).
12. Define a left primitive ideal. Define a right primitive ideal.
13. Define a left quasi-regular element. Define a right quasi-regular element.
14. (Theorem IX.2.3) State the Jacobson radical equivalences.
15. Define a semisimple ring.
16. Define a radical ring.
17. (Theorem IX.2.10) Let R be a ring. Prove that:

    (i) If R is primitive, then R is semisimple.

    (ii) If R is simple and semisimple, then R is primitive.

    (iii) If R is simple, then R is either a primitive semisimple or a radical ring.
18. Define a nilpotent ring element. Define a nilpotent ideal.
19. Define a nil ideal.
20. Is a nil ideal nilpotent? Is a nilpotent ideal nil?
21. (Theorem IX.2.14) Prove that if R is a ring, then the quotient ring $R/J(R)$ is semisimple.
22. (Exercise IX.2.2) Prove Kaplansky's Theorem: R is a division ring if and only if every element of R except one is left quasi-regular. [Note that the only element in a division ring D that is not quasi-regular is -1_D.]
23. (Exercise IX.2.4) Prove that the radical $J(R)$ contains no nonzero idempotents. However, prove that a nonzero idempotent may be left quasi-regular.
24. (Exercise IX.2.6(a)) Prove that the homomorphic image of a semisimple ring need not be semisimple.
25. (Exercise IX.2.6(b)) Prove that if $f : R \to S$ is a ring epimorphism, then $f(J(R)) \subset J(S)$.

26. (Exercise IX.2.17) Show that Nakayama's Lemma (Theorem VIII.4.5) is valid for any ring R with identity, provided condition (i) is replaced by the condition (i') J is contained in the Jacobson radical of R.
27. Define the subdirect product.
28. (Theorem IX.3.3) State and prove the other Wedderburn-Artin Theorem.
29. Define a semisimple module.
30. Define a left Artinian K-algebra.
31. Define a left (algebra) A-module.
32. Define a left (algebra) A-submodule.
33. Define a simple left (algebra) A-module.
34. Define a (algebra) A-module homomorphism.
35. (Theorem IX.5.4) Prove that A is a semisimple left Artinian K-algebra if and only if there is an isomorphism of K-algebras
$$A \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_t}(D_t)$$
where each n_i is a positive integer and each D_i is a division algebra over K.
36. Define an algebraic algebra.
37. (Proposition IX.5.8) State and prove Maschke's Theorem.
38. Define a central simple K-algebra.
39. (Theorem IX.6.2) Prove that if A is a central simple algebra over a field K and B is a simple K-algebra with identity, then $A \otimes_K B$ is a simple K-algebra.

5.8 Chapter X - Categories

1. Define a covariant functor. Define a contravariant functor.
2. Define the covariant hom functor. Define the contravariant hom functor.
3. Define a natural transformation. Define a natural isomorphism / equivalence.
4. Define a representable covariant functor. Define a representable contravariant functor.
5. (Theorem X.1.6) Let $T : \mathscr{C} \to \mathscr{S}$ be a covariant functor from a category $\mathscr{C}$ to the category $\mathscr{S}$ of sets. Prove that there is a one-to-one correspondence between the class X of all representations of T and the class Y of all universal elements of T, given by $(A, \alpha) \mapsto (A, \alpha_A(1_A))$.
6. Define an adjoint pair.
7. (Proposition X.2.2) Prove that a covariant functor $T : \mathscr{D} \to \mathscr{C}$ has a left adjoint if and only if for each object C in $\mathscr{C}$ the functor $\hom_{\mathscr{C}}(C, T(-)) : \mathscr{D} \to \mathscr{S}$ is representable.
8. Define a monic morphism.
9. Define an epic morphism.
10. Define a zero object.

Index