MATH 31 – HOMEWORK 8 SOLUTIONS!

due Wednesday, August 23

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. Let R be a commutative ring with unity (i.e., with a 1) and suppose $a, b \in R$.

   (a) Prove that if ab is a unit, then both a and b are units.

   (b) Prove that if ab is a zero-divisor, then either a is a zero-divisor or b is a zero-divisor.

   (c) Suppose R is a domain. Prove that if $a, b \in R$ are such that $a^2 = b^2$, then $a = b$ or $a = -b$.

   Proof of (a): Suppose that ab is a unit. By definition, this implies that there exists a unit $u \in R$ such that $(ab)u = 1_R$ and $u(ab) = 1_R$. (As R is commutative, these two pieces of information are equivalent.)

   Since $u(ab) = 1_R$ and R is commutative, it follows that

   $$a(ub) = (ub)a = 1_R,$$

   proving that a is a unit. Similarly,

   $$b(ua) = (ua)b = 1_R,$$

   proving that b is a unit. □

   Proof of (b): Suppose that ab is a zero-divisor. By definition, this implies that there exists a non-zero element $z \in R$ such that $(ab)z = 0_R$ or $z(ab) = 0_R$. (Again, R is commutative, so these are really the same.)

   Now observe that $a(bz) = 0_R$ as well. Does this make a a zero-divisor? Not automatically! In order for a to be a zero-divisor, we must have $bz \neq 0$.

   First, let us point out that if either a or b is itself 0, then the theorem is true. We can thus henceforth assume that a and b are both nonzero.

   We consider two cases. First, if $bz \neq 0$, then as argued above we can conclude that a is a zero-divisor. If, on the other hand, $bz = 0$, then since we know $z \neq 0$ it follows that b is a zero-divisor. □

   Note: If you think your proof shows (or could show) that *both* a and b must be zero-divisors, then your proof must be wrong! For example, in $(\mathbb{Z}_8, \oplus, \otimes)$, the element $2 \cdot 3 = 6$ is a zero-divisor, but 3 is not.

   Proof of (c): First note that we can apply the distributive rules several times along with commutativity to see that

   $$(a+b)(a-b) = (a+b)a - (a+b)b = a^2 + ba - ab - b^2 = a^2 + b^2.$$

   (Note: every time we use the "$-$", we just mean the additive inverse of the corresponding element.)

   Under the assumption that $a^2 = b^2$, it must follow that $a^2 - b^2 = 0$, and thus

   $$(a+b)(a-b) = 0.$$

   Integral domains have no non-trivial zero-divisors. This implies that if the product of two elements is zero, then one of the elements must itself be zero. So, either $a + b = 0$, in which case $a = -b$, or else $a - b = 0$ in which case $a = b$. □

---

2. (16.7) Let X be a set and let $R = \mathcal{P}(X)$.

   (a) Show that $(R, \triangle, \cap)$ is a ring, where $\triangle$ denotes the symmetric difference and $\cap$ denotes the intersection.

   (b) A *Boolean ring* is one in which every element a has the property that $a^2 = a$. Show that $(R, \triangle, \cap)$ is a Boolean ring.

   Proof of (a): To show that $R = (\mathcal{P}(X), \triangle, \cap)$ is a ring, we need to verify that

   - $(\mathcal{P}(X), \triangle)$ is an abelian group,
   - $\cap$ is associative
   - the distributive laws hold, i.e.,

   $$S_1 \cap (S_2 \triangle S_3) = (S_1 \cap S_2) \triangle (S_1 \cap S_3) \qquad \text{and} \qquad (S_2 \triangle S_3) \cap S_1 = (S_2 \cap S_1) \triangle (S_3 \cap S_1).$$

   We proved way back in the first homework that $(\mathcal{P}(X), \triangle)$ is a group—clearly an abelian one by the definition of $\triangle$.

   The associativity of $\cap$ is easy to see:

   $$\begin{aligned} R \cap (S \cap T) &= \{x : x \in R \text{ and } x \in S \cap T\} \\ &= \{x : x \in R, x \in S, x \in T\} \\ &= \{x : x \in R \cap S \text{ and } x \in T\} \\ &= (R \cap S) \cap T. \end{aligned}$$

   Moreover, $\cap$ is a commutative operation. This means we only need to check one of the distributive laws, as the other follows by commutativity.

   Let's dive in and see if we can prove it. Suppose that $x \in S_1 \cap (S_2 \triangle S_3)$. This implies that $x \in S_1$ and either $x \in S_2 \smallsetminus S_3$ or $x \in S_3 \smallsetminus S_2$ (but not both). If $x \in S_2 \smallsetminus S_3$, then $x \in S_1 \cap S_2$ and $x \notin S_1 \cap S_3$. If $x \in S_3 \smallsetminus S_2$, then $x \in S_1 \cap S_3$ and $x \notin S_1 \cap S_2$. This proves that $x \in (S_1 \cap S_2) \triangle (S_1 \cap S_3)$.

   Conversely, suppose that $x \in (S_1 \cap S_2) \triangle (S_1 \cap S_3)$. Then, x is in either $S_1 \cap S_2$ or $S_1 \cap S_3$, but not both. Either way, we must have $x \in S_1$.

   If $x \in S_1 \cap S_2$ and $x \notin S_1 \cap S_3$, then $x \in S_1$, $x \in S_2$, $x \notin S_3$, proving that $x \in S_1 \cap (S_2 \triangle S_3)$. Otherwise, we must have $x \in S_1 \cap S_3$ and $x \notin S_1 \cap S_2$, in which case $x \in S_1$, $x \notin S_2$, $x \in S_3$, proving again that $x \in S_1 \cap (S_2 \triangle S_3)$.

   This proves the distributive rule, and completes the proof that R is a (commutative ring). (Note: R also has a 1—the set X itself.) □

   Proof of (b): This is trivially true! Let $S \subseteq X$. Then $S \cap S = S$. If you insist on a more formal justification,

   $$S \cap S = \{x : x \in S \text{ and } x \in S\} = \{x : x \in S\} = S.$$

   Hence, R is Boolean. □

---

3. (17.7) Find all the maximal ideals in the ring $(\mathbb{Z}_n, \oplus, \otimes)$.

   Solution: In order to convince yourself that an ideal is maximal, it usually helps to know what *all* the ideals look like. So, first we'll describe the set of *all ideals*. Then we'll identify the ones of those that are maximal.

   We can use our knowledge of group theory to help us. Any ideal of the ring $(\mathbb{Z}_n, \oplus, \otimes)$ must also be, by the definition of an ideal, a subgroup of $(\mathbb{Z}_n, \oplus)$. We've previously identified the distinct subgroups of $(\mathbb{Z}_n, \oplus)$: they are all of the form $\langle \ell \rangle$, where ℓ divides n. For example, the subgroups of $(\mathbb{Z}_{20}, \oplus)$ are

   $$\langle 1 \rangle, \quad \langle 2 \rangle, \quad \langle 4 \rangle, \quad \langle 5 \rangle, \quad \langle 10 \rangle, \quad \langle 20 \rangle.$$

Moreover, these are all distinct. The first item in this list is the whole group, and the last item is the subgroup containing only the identity. Since we don't use the "cyclic subgroup" notation for rings, we can alternately call these subgroups

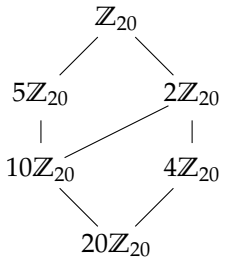
$$1\mathbb{Z}_{20}, \quad 2\mathbb{Z}_{20}, \quad 4\mathbb{Z}_{20}, \quad 5\mathbb{Z}_{20}, \quad 10\mathbb{Z}_{20}, \quad 20\mathbb{Z}_{20}.$$

Since all ideals are additive subgroups, we now have a list of candidates to look at. It turns out that for the ring $(\mathbb{Z}_n, \oplus, \otimes)$ all of the additive subgroups are ideals. Why? Suppose ℓ divides n and consider $\ell\mathbb{Z}_n$. We only need to check that if $x \in \ell\mathbb{Z}_n$ and $y \in \mathbb{Z}_n$, then $xy \in \ell\mathbb{Z}_n$, but this is clearly true because $\ell\mathbb{Z}_n$ consists of all the multiples (mod n) of ℓ.

Now, we have confirmed that the set of all distinct ideals of $(\mathbb{Z}_n, \oplus, \otimes)$ is

$$\{\ell\mathbb{Z}_n : \ell \text{ divides } n\}.$$

We can draw an ideal lattice based on subset containment just like we did for subgroups. For $(\mathbb{Z}_{20}, \oplus, \otimes)$, as an example:



For this example we can plainly see the maximal ideals: $2\mathbb{Z}_{20}$ and $5\mathbb{Z}_{20}$. Here's the general claim that we'll prove: the distinct maximal ideals of $(\mathbb{Z}_{20}, \oplus, \otimes)$ are

$$S = \{\ell\mathbb{Z}_n : \ell \text{ divides } n \text{ and } \ell \text{ is a prime number}\}.$$

By our argument so far, every element of S is an ideal. We need to check that each is maximal. Let $p\mathbb{Z}_n \in S$, and suppose there is another ideal J that properly contains $p\mathbb{Z}_n$. We now know that J must have the form $k\mathbb{Z}_n$ where k is an integer that divides p evenly. As p is prime, the only such integers are 1 and k, proving that J must be all of $\mathbb{Z}_n$. Hence, every element of S is a maximal ideal.

We also need to argue that we haven't missed any of the prime ideals. Let $\ell\mathbb{Z}_n$ be an ideal not in S. Then, by the definition of S, ℓ is not prime. Also ℓ divides n evenly. So, we can write ℓ as $m_1 \cdot m_2$ where m_1 and m_2 both divide n evenly as well (and are bigger than 1). It must then be the case that $m_1\mathbb{Z}_n$ is an ideal that is not the whole ring, and properly contains $\ell\mathbb{Z}_n$, proving that $\ell\mathbb{Z}_n$ is not maximal.

Note that these arguments are all possible because the first thing we did is classify *all* of the ideasls.

---

4. (17.10) Let X be a nonempty set and let R be the ring $(\mathcal{P}(X), \triangle, \cap)$.

   (a) Show that if $Y \subsetneq X$ (this symbol means that Y is a subset of X and $Y \neq X$), then $\mathcal{P}(Y)$ is an ideal in R and has a multiplicative identity different from that of R.

   (b) Find a maximal ideal in R.

Proof of (a): Let $Y \subsetneq X$. To show that $\mathcal{P}(Y)$ is an ideal in R, we need to show that $(\mathcal{P}(Y), \triangle)$ is an abelian subgroup, and that for all $S \in \mathcal{P}(Y)$ and $T \in \mathcal{P}(X)$ we have $S \cap T \in \mathcal{P}(Y)$.

In Homework 1, we proved that $(\mathcal{P}(Z), \triangle)$ is a group for any Z. As stated in the solution to problem 2 of this assignment, $\triangle$ is by its definition a commutative operation.

Now let $S \in \mathcal{P}(Y)$ and $T \in \mathcal{P}(X)$. It follows that $S \cap T \subseteq S$ (this is true for any sets ever), and since $S \subseteq Y$ we have $S \cap T \in \mathcal{P}(Y)$. This confirms that if $Y \subsetneq X$ then $\mathcal{P}(Y)$ is an ideal of $\mathcal{P}(X)$. It *does not prove* that these are the only ideals.

If we're going to show that the multiplicative identity of $\mathcal{P}(Y)$ is different from that of $\mathcal{P}(X)$, we need to first figure out what the multiplicative identity of $\mathcal{P}(X)$ even is. I claim that it's the set X itself. This is easy to check: for any $S \in \mathcal{P}(X)$,

$$S \cap X = S.$$

As the multiplicative identity is unique, it must be X.

What is the multiplicative identity in the ideal $\mathcal{P}(Y)$? It's certainly not X because X is not even an element of $\mathcal{P}(Y)$. By the same logic, the multiplicative identity is Y itself: for any $S \in \mathcal{P}(Y)$,

$$S \cap Y = S.$$

□

Proof of (b): Let $a \in X$. I claim that $\mathcal{P}(X \setminus \{a\})$ is a maximal ideal of $\mathcal{P}(X)$. We know for sure that $\mathcal{P}(X \setminus \{a\})$ is an ideal (part (a) proves this). Suppose that J is an ideal of $\mathcal{P}(X)$ that properly contains $\mathcal{P}(X \setminus \{a\})$. We *do not know* that J has the form $\mathcal{P}(S)$ for some $S \subseteq X$, unless you proved in part (a) that *every* ideal has the form. However, we do know that J must contain one element that is a set that contains a, because if every set in J did not contain a, then J would be contained in $\mathcal{P}(X \setminus \{a\})$. We will show that J must be the whole ring $\mathcal{P}(X)$. Let T be the set in J that contains a.

Because J is an ideal, it must be true that

$$T \cap \{a\} \in J,$$

and since $T \cap \{a\} = \{a\}$ we can now conclude that $\{a\} \in J$.

Every subset of S either contains a or doesn't contain a. If it doesn't contain a, then it's in $\mathcal{P}(X \setminus \{a\})$ and hence also in J. If S does contain a, then

$$S \setminus \{a\} \in \mathcal{P}(X \setminus \{a\}) \subseteq J,$$

and

$$\{a\} \in J,$$

so

$$S = (S \setminus \{a\}) \triangle \{a\} \in J.$$

This shows that every subset of X is contained in J, implying that $J = \mathcal{P}(X)$. Hence, $\mathcal{P}(X \setminus \{a\})$ is maximal. □

---

5. (18.14) Let $\varphi : R \to S$ be a ring homomorphism and suppose that S has a multiplicative identity 1_S. Show that $\varphi^{-1}(\{1_S\})$ is an ideal in R if and only if S is trivial.

Proof:
($\Longleftarrow$) Suppose S is trivial. Then, S contains only one element, which is both the 0 and the 1. The map φ must send *everything* in R somewhere, and the only place to be sent is $0_S = 1_S$. Therefore $\varphi^{-1}(\{1_S\}) = R$, and any ring is always an ideal in itself.

($\Longrightarrow$) Suppose $\varphi^{-1}(\{1_S\})$ is an ideal in R, and call this ideal I. Every ideal contains the additive identity of the ring, i.e., $0_R \in I$. Therefore, by the definition of I, we know

$$\varphi(0_R) = 1_S.$$

On the other hand, it is a rule for any homomorphism that

$$\varphi(0_R) = 0_S.$$

Therefore $1_S = 0_S$ and we saw in class that this is only possible if S is the trivial ring consisting of only a single element.
