Modern Algebra Homework Batch 5

The previous homework batch (Batch 4) dealt with the basics of ring theory, including an introduction to ideals and quotient rings. As there were quite a few problems in this batch dealing with the concept of “ideal,” I should probably remind everyone once again as to the “template” demonstrating that a given subset $I \subseteq R$ is an ideal of $R$.

**Problem:** To show that a given subset $I \subseteq R$ is an ideal.

**Solution:** One must show that

1. $(I, +)$ is a subgroup of $(R, +)$. To do this one must show that
   
   (a) $x, y \in I$ implies that $x + y \in I$;
   
   (b) $0 \in I$;
   
   (c) $x \in I$ implies that $-x \in I$.

2. $I$ satisfies the “super-absorption” law: that is, one must show that if $x \in I$ and if $r \in R$, then $rx \in I$ and $xr \in I$.

In the last homework batch, some of you were confusing addition with multiplication. Again, one is to show that $I \subseteq R$ is a subgroup with respect to *addition* rather than with respect to multiplication.

Actually we can simplify the above template considerably. Let me state the result as follows:

**Proposition.** Let $R$ be a ring and let $I \subseteq R$. Then $I$ is an ideal of $R$ if and only if $I$ is closed under addition and satisfies super-absorption.

**Proof.** Obviously, if $I$ is an ideal of $R$, then $I$ is closed under addition and satisfies super-absorption. Thus, we assume that $I$ is closed under addition and is closed under super-absorption. Obviously, the only things we need to check are that $0 \in I$ and that $I$ is closed under taking additive inverses. To see this, start by taking any element $x \in I$ and observe that $0 = 0 \cdot x \in I$ (by super-absorption). This proves already that $0 \in I$. Finally, if $x \in I$, note that $-x = (-1)x \in I$, again by super-absorption. This proves the proposition.

The above shows the power of the super-absorption law. Furthermore, it now provides a simplified template for checking that a given subset $I \subseteq R$ is an ideal:

**Problem:** To show that a given subset $I \subseteq R$ is an ideal.
Solution: One need only show that

1. $I$ is closed under addition.

2. $I$ is closed under “super-absorption” law, that is, $x \in I$ and if $r \in R$, then $rx \in I$ and $xr \in I$.

In the present batch of problems, we will consider some of the concepts that are important to so-called factorization theory: prime ideals, maximal ideals, and polynomial rings. These concepts will draw from Sections 4.5 and 6 of Chapter 4 in the text. At the end of (4.5) a very important (but inconspicuously displayed) definition is given: that of a Euclidean domain. Such rings are very central to factorization theory, and provide a very conceptual and unified framework for the “Fundamental Theorem of Arithmetic.”

Consider the following exercises:


Discussion: The above exercises all stem from Examples 1-4 (pp. 149-150) in the text. You should spend a good deal of time with these examples. Note that Exercise 5 asks you to prove that $R/I \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$. For “categorical” reasons, I’d rather you write $\mathbb{Z}_5 \times \mathbb{Z}_5$—for your purposes, they’re the same ring, though. As a hint for problems 3,4, let me suggest the following. In this case $R$ is the ring

$$R = \{a + bi \mid a, b \in \mathbb{Z}\};$$

define $\phi : R \to \mathbb{Z}_5$ by setting $\phi(a + bi) = [a + 2b]_5 \in \mathbb{Z}_5$. Verify that $\phi$ is a surjective ring homomorphism. Thus, by the Fundamental Homomorphism Theorem we get $R/\ker \phi \cong \mathbb{Z}_5$. Now show that $\ker \phi = I = \{x(2 + i) \mid x \in R\}$. Since $\mathbb{Z}_5$ is a field, this automatically implies that $I$ is a maximal ideal of $R$.

Anyway, give this some thought.

Further Remarks: One page 148, it is said that Section 4 is a section with only one major theorem. I think that one should include two major theorems (I’ll write them below); indeed they very much go hand in hand. First, let me remind you of two important definitions.

Definition [prime ideal]. Let $R$ be a commutative ring and let $P \subseteq R$, $P \neq R$ be an ideal. We say that $P$ is a prime ideal if whenever the product $ab \in P$, $a, b, \in R$, then either $a \in P$ or $b \in P$ (or both).
**Definition** [maximal ideal]. Let $R$ be a commutative ring and let $M \subseteq R$, $M \neq R$ be an ideal. We say that $M$ is a maximal ideal if the only ideals of $R$ containing $M$ are $M$ and $R$ itself.

**Theorem.** Let $R$ be a commutative ring, and let $P \subseteq R$ be an ideal. Then $P$ is a prime ideal if and only if $R/P$ is an integral domain.

**Theorem.** Let $R$ be a commutative ring, and let $M \subseteq R$ be an ideal. Then $M$ is a prime ideal if and only if $R/M$ is a field.

Since we have already seen that a field is an integral domain, the following is immediate:

**Corollary.** Let $R$ be a commutative ring, and let $M \subseteq R$ be a maximal ideal. Then $M$ is a prime ideal.

(4. 5), p. 163: 1,3, 6, 10. Also, do these:

(A) Let $F$ be a field, and let $F[x]$ be the ring of polynomials over $F$. Fix an element $\alpha \in F$, and define the evaluation homomorphism ("plugging in") by setting

$$E_\alpha : F[x] \to F, \quad E_\alpha(f(x)) = f(\alpha).$$

In the above, if $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i$. Show that $E_\alpha$ is a ring homomorphism $F[x] \to F$. (While this exercise is entirely routine, it is a bit tedious.)

(B) Let $F$ be a field, and let $F[x]$ be the ring of polynomials over $F$. Let $f(x) \in F[x]$ and let $\alpha \in F$. Show that

$$f(x) = (x - \alpha)q(x) + f(\alpha),$$

for some polynomial $q(x) \in F[x]$, and where $f(\alpha) = E_\alpha(f(x))$.

(C) Let $F$ be a field, and let $F[x]$ be the ring of polynomials over $F$. If $\alpha \in F$, and $f(x) \in F[x]$, we say that $\alpha$ is a root of $f(x)$ if and only if $f(\alpha) = 0$, i.e., if and only if $E_\alpha(f(x)) = 0$. Prove that $\alpha$ is a root of $f(x)$ if and only if $(x - \alpha) \mid f(x)$.

(D) (This is really problem #13, p. 164, put into a better context.) Let $\mathbb{R}, \mathbb{C}$ be the real and complex fields, respectively. Prove that there is an isomorphism $F[x]/(x^2+1) \cong \mathbb{C}$. (Use the evaluation homomorphism $x \mapsto i$, and apply the Fundamental Homomorphism Theorem.)
(E) Let $F$ be a field, and let $f(x) \in F[x]$. If $f(x)$ is reducible, and has degree less than or equal to 3, prove that $f(x)$ has a root in $F$.

(F) Prove the so-called Fundamental Theorem of College Algebra: Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$ be a polynomial with integer coefficients. If $\alpha = \frac{a}{b} \in \mathbb{Q}$ (rational field) is a root of $f(x)$ where $(a, b) = 1$, show that $a|a_0$ and $b|a_n$. (Hint: plug $\alpha$ into $f(x)$ and multiply everything by $b^n$.)

(4. 6), p. 171: 2, 5 (mimick the treatment given in Example 5, on page 170). Also try the following:

(A) Let $\mathbb{Z}[x]$ be the polynomial ring over the ring $\mathbb{Z}$ of integers, and let $p$ be a prime number. If $\mathbb{Z}_p$ is the ring of integers modulo $p$, we may define a map $\theta : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ be setting $\theta(f(x)) = \bar{a} f(x)$, where if $f(x) = \sum_{i=0}^{n} a_i x^i$, then $\bar{f}(x) = \sum_{i=0}^{n} [a_i]_p x^i \in \mathbb{Z}_p[x]$. Show that $\theta : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ is a ring homomorphism.

(B) Let $f(x) \in \mathbb{Z}[x]$, and let $p$ be a prime. Show that if $\bar{f}(x) \in \mathbb{Z}_p[x]$ is irreducible, so is $f(x)$.

(C) Let $f(x) = x^6 + x + 1 \in \mathbb{Z}[x]$. Show that $f(x)$ is irreducible. (Hint: Show that $\bar{f}(x) \in \mathbb{Z}_2[x]$ is irreducible. This really is very easy; for suppose, by way of contradiction that $\bar{f}(x)$ is reducible. Since $\bar{f}(x)$ clearly has no roots in $\mathbb{Z}_2$, then $\bar{f}(x)$ must have an irreducible quadratic or an irreducible cubic as a factor. However, it is easy to show that the only irreducible quadratic of $\mathbb{Z}_2[x]$ is $x^2 + x + 1$ and that the only irreducible cubics of $\mathbb{Z}_2[x]$ are $x^3 + x^2 + 1$ and $x^3 + x + 1$, none of which divide $\bar{f}(x)$ in $\mathbb{Z}_2[x]$ (try the long division). )