Math 31 – Homework 7

Note: This assignment is optional.

Note: Any problem labeled as "show" or "prove" should be written up as a formal proof, using complete sentences to convey your ideas.

Basic Ring Theory

The problems on this list all involve basic definitions and examples of rings, along with ring homomorphisms. You should be able to do them all after the x-hour on August 13.

1. Let R be an integral domain. If $a, b, c \in R$ with $a \neq 0$ and $ab = ac$, show that $b = c$.

Proof. If $ab = ac$, then $ab - ac = 0$, and the left distributive law gives

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

Since R is an integral domain and $a \neq 0$, we must have $b - c = 0$. In other words, $b = c$. □

2. Find the following products of quaternions.

(a) $(i+j)(i-j)$.

(b) $(1-i+2j-2k)(1+2i-4j+6k)$.

(c) $(2i-3j+4k)^2$.

(d) $i(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)-(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)i$.

Solution. (a) We have

$$\begin{aligned}(i+j)(i-j) &= i(i-j)+j(i-j)\\ &= i^2-ij+ji-j^2\\ &= -1-k-k-(-1)\\ &= -2k.\end{aligned}$$

(b) In this case we have

$$\begin{aligned}(1-i+2j-2k)(1+2i-4j+6k) &= 1+2i-4j+6k\\ &\quad - i-2i^2+4ij-6ik\\ &\quad + 2j+4ji-8j^2+12jk\\ &\quad - 2k-4ki+8kj-12k^2\\ &= 1+i-2j+4k+2+2j+8+4i+12\\ &= 23+5i+4k.\end{aligned}$$

(c) If we square this quaternion, we get

$$\begin{aligned}(2i-3j+4k)^2 &= -4-9-16-6ij-6ji+8ik+8ki-12jk-12kj \\ &= -29.\end{aligned}$$

(d) Finally, we have

$$\begin{aligned}i(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)-(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)i &= \alpha_2 ij-\alpha_2 ji+\alpha_3 ik-\alpha_3 ki \\ &= 2\alpha_2 k-2\alpha_3 j.\end{aligned}$$

3. Let R be a commutative ring with identity. Show that if $u \in R$ is a unit, then u is not a zero divisor. Conclude that any field is necessarily an integral domain. [**Note:** This is proven in Corollary 16.3 of Saracino if you'd like to check your answer there.]

Proof. Let $a \in R$ be a unit, and suppose that there is a $b \in R$ such that $ab = 0$. Then

$$a^{-1}(ab) = a^{-1} \cdot 0 = 0.$$

But $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$, so we must have $b = 0$. Therefore, a is not a zero divisor.

4. Let R be a finite integral domain with identity $1 \in R$. Show that R is actually a field. [**Note:** This is Theorem 16.7 in Saracino.]

Proof. We need to show that any nonzero element of R has a multiplicative inverse, i.e., that it is a unit. Since R is finite, we can list out the elements of R:

$$R = \{0, 1, a_1, a_2, \ldots, a_n\}$$

for some $n \in \mathbb{Z}$. In problem 1, you proved that if $ab = ac$ for some $b, c \in R$, then $b = c$. Therefore, the elements

$$a \cdot 0, a \cdot 1, aa_1, aa_2, \ldots, aa_n$$

must all be distinct, and since there are $n+2$ of them, these must be all the elements of R. The first is $a \cdot 0 = 0$, and the second is $a \cdot 1 = a$. Since $1 \in R$, it must appear somewhere on this list. That is, there is an i between 1 and n such that $aa_i = 1$. But then $a_i = a^{-1}$, and a is a unit. Therefore, R is a field.

5. [Saracino, #16.16] Let R be a ring. An element $r \in R$ is a (multiplicative) **idempotent** if $r^2 = r$. We say that R is a **Boolean ring** if every element of R is a multiplicative idempotent. If R is Boolean, show that

(a) $2r = 0$ for every $r \in R$ (i.e., $r = -r$).

Proof. Let $r \in R$. Then we have

$$(-r)^2 = (-r)(-r) = r \cdot r = r^2 = r.$$

On the other hand,

$$(-r)^2 = -r$$

since R is Boolean. Therefore, $r = -r$.

(b) R is commutative.

Proof. Let $a, b \in R$, and consider $(a+b)^2$:

$$(a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b,$$

since R is Boolean. On the other hand, $(a+b)^2 = a+b$, so

$$a + ab + ba + b = a + b.$$

Subtracting a and b from both sides, we have

$$ab + ba = 0,$$

so $ab = -ba$. But we saw in part (a) that $-ba = ba$, so it follows that $ab = ba$. Therefore, R is commutative.

6. Let R and S be two rings with identity, and let 1_R and 1_S denote the multiplicative identities of R and S, respectively. Let $\varphi : R \to S$ be a nonzero ring homomorphism. (That is, φ does not map every element of R to 0.)

(a) Show that if $\varphi(1_R) \neq 1_S$, then $\varphi(1_R)$ must be a zero divisor in S. Conclude that if S is an integral domain, then $\varphi(1_R) = 1_S$.

Proof. If $\varphi(1_R) \neq 1_S$, then $\varphi(1_R) - 1_S \neq 0$. However, if we multiply this by $\varphi(1_R)$, we get

$$\varphi(1_R)\left(\varphi(1_R) - 1_S\right) = \varphi(1_R)\varphi(1_R) - \varphi(1_R) \cdot 1_S = \varphi(1_R) - \varphi(1_R) = 0.$$

Therefore, $\varphi(1_R)$ is a zero divisor. If S is an integral domain, it has no zero divisors, and we must have $\varphi(1_R) = 1_S$ in this case.

(b) Prove that if $\varphi(1_R) = 1_S$ and $u \in R$ is a unit, then $\varphi(u)$ is a unit in S and

$$\varphi(u^{-1}) = \varphi(u)^{-1}.$$

Proof. Let u be a unit in R. Then

$$\varphi(u)\varphi(u^{-1}) = \varphi(uu^{-1}) = \varphi(1_R) = 1_S.$$

Similarly, $\varphi(u^{-1})\varphi(u) = 1_S$, so $\varphi(u)$ is a unit with $\varphi(u)^{-1} = \varphi(u^{-1})$.

Ideals and Polynomials

The following questions deal with ideals, quotient rings, and polynomial rings. You should be able to complete them after class on Monday, August 19.

1. Let R be a ring, and suppose that I and J are ideals in R. Prove that $I \cap J$ is an ideal in R.

Proof. Since I and J are subgroups of the abelian group $\langle R, + \rangle$, we already know that $I \cap J$ is an additive subgroup of R. Suppose then that $a \in I \cap J$ and $r \in R$. Then $a \in I$ and $a \in J$, so $ra \in I$ and $ra \in J$, since I and J are both ideals. Similarly, $ar \in I$ and $ar \in J$, so $ra, ar \in I \cap J$. Therefore, $I \cap J$ is an ideal of R.

2. Let R be a commutative ring. An element $a \in R$ is said to be **nilpotent** if there is a positive integer n such that $a^n = 0$. The set

$$\text{Nil}(R) = \{a \in R : a \text{ is nilpotent}\}$$

is called the **nilradical** of R. Prove that the nilradical is an ideal of R. [**Hint:** You may need to use the fact that the usual binomial theorem holds in a commutative ring. That is, if $a, b \in R$ and $n \in \mathbb{Z}^+$, then

$$(a+b)^n = \sum_{k=0}^{n} a^{n-k} b^k.$$

This should help with checking that $\text{Nil}(R)$ is closed under addition.]

Proof. We first show that $\text{Nil}(R)$ is closed under addition. If $a, b \in \text{Nil}(R)$, then there are integers n and m such that $a^n = 0$ and $b^m = 0$. We then claim that $(ab)^{nm} = 0$. To see this, we use the binomial expansion of $(a+b)^{nm}$:

$$(a+b)^{nm} = \sum_{k=0}^{nm} a^{nm-k} b^k.$$

Note that if $k \geq m$, then $b^k = 0$, so we really only have

$$(a+b)^{nm} = \sum_{k=0}^{m-1} a^{nm-k} b^k.$$

But for $k < m$, $nm - k \geq nm - (m-1) = (n-1)m + 1 \geq n$, so $a^{nm-k} = 0$ when $k < m$. Therefore, $(a+b)^{nm} = 0$, as claimed. Of course if $a \in \text{Nil}(R)$, then $-a$ is as well, and $0 \in \text{Nil}(R)$, so $\text{Nil}(R)$ is an additive subgroup of R.

It remains to show that if $a \in \text{Nil}(R)$ and $r \in R$, then $ra \in \text{Nil}(R)$. Suppose that $a^n = 0$. Then since R is commutative, we have

$$(ra)^n = r^n a^n = r^n \cdot 0 = 0.$$

Thus ra is nilpotent, and $\text{Nil}(R)$ is an ideal of R.

3. [Saracino, #17.14] Let R be a ring and I an ideal of R.

(a) If R is commutative, show that R/I is commutative.

Proof. Let $R + a$ and $R + b$ be elements of R/I. Then

$$(R + a)(R + b) = R + (ab) = R + (ba) = (R + b)(R + a),$$

so R/I is commutative.

(b) If R has an identity, show that R/I also has an identity.

Proof. We claim that $R+1$ is the identity in R/I. To see this, note that if $R+a \in R/I$, then

$$(R + 1)(R + a) = R + (1 \cdot a) = R + a,$$

and similarly $(R + a)(R + 1) = R + a$.

4. Determine whether each of the following polynomials is irreducible over the given field.

(a) $3x^4 + 5x^3 + 50x + 15$ over $\mathbb{Q}$.

Solution. This is irreducible by Eisenstein's criterion: the prime 5 divides every coefficient except the leading one, and $5^2 = 25$ doesn't divide the constant term 15, so the polynomial is irreducible over $\mathbb{Q}$.

(b) $x^2 + 7$ over $\mathbb{Q}$.

Solution. This is also irreducible by Eisenstein. Since 7 divides the constant term but not the leading coefficient and $7^2 = 49$ does not divide the constant term, it is irreducible over $\mathbb{Q}$.

(c) $x^2 + 7$ over $\mathbb{C}$.

Solution. This polynomial is not irreducible over $\mathbb{C}$. It has roots $\pm i\sqrt{7}$ in $\mathbb{C}$, so it factors as

$$x^2 + 7 = (x + i\sqrt{7})(x - i\sqrt{7}).$$