Math 411: Honors Algebra I
Problem Set 10
due: November 29, 2017

Emily Riehl

Exercise 1. Let $R$ be a commutative ring.

(i) Prove that if $I \subset R$ is an ideal and $1 \in I$ then $I = R$.

(ii) Prove that the only ideals in a field are the zero ideal $I = \{0\}$ or the ideal containing every element.

(iii) Prove that every ring homomorphism $\mathbb{k} \to K$ between fields is an injection by arguing that the kernel must be zero.

Proof.
(i) If $1 \in I$ then $r \cdot 1 = r \in I$ for all $r \in R$ so $I = R$.

(ii) Let $I$ be an ideal contained in a field. If $I \neq 0$ then $I$ contains some non-zero element $x$. But then by multiplication stability $x^{-1} \cdot x = 1 \in I$ and so by (i) the ideal equals the entire field.

(iii) Every ring homomorphism has a kernel, which is then an ideal of the domain ring. If the kernel were the entire ring, then the homomorphism would send $1$ to $0$, which can’t happen since $1 \neq 0$ in every field. So the kernel must be zero, which means the homomorphism is injective.

Exercise 2.

(i) The subset $\mathbb{Z} \subset \mathbb{Z}[x]$ of constant polynomials is a subgroup under addition but is not an ideal. Nonetheless we can form the quotient group $\mathbb{Z}[x]/\mathbb{Z}$. The cosets $f(x) + \mathbb{Z}$ are represented by polynomials $f(x) = a_1 x + \cdots + a_n x^n$ with no constant term. Prove that the formula

$$(f(x) + \mathbb{Z}) \cdot (g(x) + \mathbb{Z}) := (f(x) \cdot g(x)) + \mathbb{Z}$$

is not well-defined by finding explicit polynomials in the same cosets that have products that do not belong to the same cosets.

(ii) Now let $I$ be an ideal in a commutative ring $R$. Prove that the formula

$$(a + I) \cdot (b + I) := (a \cdot b) + I$$

defines a well-defined operation on the abelian group $R/I$ of cosets of $I$. This proves that $R/I$ inherits the structure of a ring in a unique way making the canonical projection $\pi: R \to R/I$ into a ring homomorphism.

Proof. (i) The polynomials $x$ and $x + 1$ are in the same coset because they are the same except for having a constant term. But $x \cdot x = x^2$ while $(x + 1) \cdot (x + 1) = x^2 + 2x + 1$ are in different cosets, since they also differ in the linear term.

(ii) We must show that if $a + I = a' + I$ and $b + I = b' + I$ then $(a \cdot b) + I = (a' \cdot b') + I$.

To say that $a + I = a' + I$ means that $a - a' \in I$. Then by multiplication stability $a \cdot b - a' \cdot b \in I$. Similarly we know that $b - b' \in I$ so by multiplication stability $a' b - a' b' \in I$. Since $I$ is a subgroup under $+$ we have that $ab - a'b + a'b - a'b' \in I$ so $ab - a'b' \in I$, which is what we wanted to show.

Exercise 3.

1 This is why ideals $I \subset R$ do not define subrings. Most ideals do not contain $1$.

2 An injective ring homomorphism $\mathbb{k} \to K$ defines a field extension of $\mathbb{k}$.
(i) Let \( a \in R \) be any element in a commutative ring. Prove that \( (a) = \{a \cdot r \mid r \in R\} \) is an ideal. This is called the principal ideal generated by \( a \).

(ii) If \( u \) is a unit prove that \( (u) = (1) = R \).

(iii) If \( a = ub \) and \( u \) is a unit prove that \( (a) = (b) \).

(iv) If \( (a) = (b) \) and \( R \) is an integral domain prove that there exists a unit \( u \) so that \( a = ub \).

**Proof.** (i) First we must show that \( (a) \) is a subgroup under addition. Note that \( a \cdot 0 = 0 \in (a) \). If \( b, c \in (a) \) this means there exist \( r, s \in R \) so that \( b = ar \) and \( c = ar \). Then \( b + c = a(r + s) \in (a) \). Similarly \( -b = a(-r) \in (a) \) also.

Finally we must show that for \( c \in (a) \) and \( r \in R \) that \( r \cdot c \in (a) \). But \( c \in (a) \) means there exists \( s \in R \) so that \( c = as \). Now \( r \cdot c = ras = a(rs) \) — since our ring is commutative, which proves that \( r \cdot c \in (a) \).

(ii) If \( u \) is a unit then there exists \( v \in R \) with \( uv = 1 \). Thus \( 1 \in (u) \) and exercise 1 proves that \( (u) = (1) = R \).

(iii) If \( a = ub \) and \( u \) is a unit then \( b = u^{-1}a \). This proves that \( (a) \subset (b) \) and \( (b) \subset (a) \) so the ideals are equal.

(iv) If \( a \in (b) \) then there is some element \( r \in R \) so that \( a = rb \). Similarly if \( b \in (a) \) there is an element \( s \in R \) so that \( b = sa \). So now \( a = rsa \), so \( 0 = a - rsa = (1 - rs)a \).

Since \( a \) is tacitly assumed to be non-zero (otherwise the integral domain hypothesis implies that \( a \) and \( b \) are both zero and we can take \( 1 \) to be the unit) we must have \( 1 - rs = 0 \) so \( r \) and \( s \) are units.

**Exercise 4.** Consider the principal ideal \( (x) \subset \mathbb{Z}[x] \). Compute the quotient ring \( \mathbb{Z}[x]/(x) \).

**Proof.** There is a ring homomorphism \( \rho: \mathbb{Z}[x] \to \mathbb{Z} \) defined by evaluating every polynomial at zero. This is the same as the homorphism that forgets everything but the constant term. It is clearly surjective and its kernel is the principal ideal generated by \( (x) \) because this is the ideal containing all polynomials with zero constant term. Now the first isomorphism theorem proves that \( \mathbb{Z}[x]/(x) \cong \mathbb{Z} \).

**Exercise 5.** Consider the principal ideal \( (x^2 + 1) \subset \mathbb{R}[x] \).

(i) Define a ring homomorphism \( \phi: \mathbb{R}[x] \to \mathbb{C} \) that sends \( \mathbb{R} \subset \mathbb{R}[x] \) to \( \mathbb{R} \subset \mathbb{C} \) and sends \( x \) to \( i = \sqrt{-1} \).

(ii) Prove that the homomorphism \( \phi \) is surjective.

(iii) Prove that \( (x^2 + 1) \) is contained in the kernel of \( \phi \). In fact \( (x^2 + 1) \) is a maximal ideal so this implies that \( \ker \phi = (x^2 + 1) \).

(iv) Apply a theorem from class to prove that the quotient ring \( \mathbb{R}[x]/(x^2 + 1) \) is isomorphic to \( \mathbb{C} \).

**Proof.** (i) The ring homomorphism \( \phi \) is defined by “evaluating \( x \) at \( i \).” This produces a polynomial in \( i \) with real coefficients which evaluates to an element of \( \mathbb{C} \).

(ii) Every complex number can be written as \( a + bi \) with \( a, b \in \mathbb{R} \). So the polynomial \( a + bx \) maps under \( \phi \) to it.

(iii) Since \( i^2 + 1 = 0 \), the polynomial \( x^2 + 1 \) evaluates at \( i \) to zero and so is contained in the kernel of \( \phi \). It follows that the principal ideal generated by \( x^2 + 1 \) is also in the kernel of \( \phi \) since any multiple of this polynomial will also evaluating to zero (since \( 0 \cdot a = 0 \) in any ring).

---

3 Pick one square root of \(-1\).
(iv) By the first isomorphism theorem, if \( \phi: R \rightarrow S \) is any surjective ring homomorphism then \( R/\ker\phi \cong S \). So we must have \( \mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C} \).

\[ \square \]

**Exercise 6.** Consider the principal ideal \( (x^2 + x + 1) \in (\mathbb{Z}/2)[x] \).

(i) Prove that any polynomial \( f(x) \in (\mathbb{Z}/2)[x] \) with coefficients in \( \mathbb{Z}/2 \) is equivalent modulo \( (x^2 + x + 1) \) to a polynomial of the form \( a + bx \) with \( a, b \in \mathbb{Z}/2 \).

(ii) How many elements are in the quotient ring \( (\mathbb{Z}/2)[x]/(x^2 + x + 1) \)?

(iii) Prove that the quotient ring \( (\mathbb{Z}/2)[x]/(x^2 + x + 1) \) is a field by writing down the multiplication table and verifying that every non-zero element is a unit.

(iv) Explain what this has to do with question 4 on Problem Set 9.

**Proof.**

(i). Consider \( f(x) = a_0 + a_1 x + \cdots + x^n \) with coefficients in \( \mathbb{Z}/2 \); we’re assuming the leading coefficient is one because otherwise \( f \) has smaller degree. Consider the polynomial \( g(x) = b_n x^{n-2} + b_{n-1} x^{n-3} + \cdots + b_2 \) where \( b_n = 1 \) and inductively from the top we defined \( a_k = b_k + b_{k+1} \) (the addition defined modulo 2). Then \( f(x) - (x^2 + x + 1)g(x) \) has degree one or zero, which proves that \( f(x) \) is equivalent modulo \( (x^2 + x + 1) \) to a polynomial of the form \( a + bx \).

(ii). Since there are two choices each for \( a \) and \( b \) there are four elements in the ring \( (\mathbb{Z}/2)[x]/(x^2 + x + 1) \).

(iii). Let me give an alternative proof just for kicks. The polynomial \( x^2 + x + 1 \) has no roots in \( \mathbb{Z}/2 \) because when you evaluate at either 0 or 1 you get 1. This means that it is an irreducible polynomial which means that the ideal \( (x^2 + x + 1) \) is maximal in \( (\mathbb{Z}/2)[x] \). Hence the quotient ring \( (\mathbb{Z}/2)[x]/(x^2 + x + 1) \) is necessarily a field.

(iv). This is another way to understand the field of four elements from question 4 on Problem Set 9.

\[ \square \]