Math 562/662 **Spring 2024**
Homework 2 **Drew Armstrong**

---

1. Generalities About Ideals. Let R be a ring.

(a) Let $I \subseteq R$ be an ideal. Prove that $I = R$ if and only if I contains a unit.
(b) Prove that R is a field if and only if it has exactly two ideals: $\{0\}$ and R.
(c) Given ideals $I, J \subseteq R$, prove that $I \cap J$ and $I + J$ are also ideals.
(d) Given elements $a_1, \ldots, a_n \in R$, prove that the set of R-*linear combinations*

$$a_1R + \cdots + a_nR := \{a_1r_1 + \cdots + a_nr_n : r_1, \ldots, r_n \in R\}$$

is the smallest ideal of R that contains the set $\{a_1, \ldots, a_n\}$.

(a): First suppose that $I = R$. Then we have $1 \in I$, so I contains a unit. Conversely, suppose that $u \in I$ for some unit $u \in R^\times$. Then for all $a \in R$ we have

$$u \in I \text{ and } u^{-1}a \in R \quad \Longrightarrow \quad a = u(u^{-1}a) \in I.$$

This implies that $R \subseteq I$ and hence $I = R$.

(b): First suppose that R is a field and consider and consider any ideal $I \subseteq R$. If $I \neq \{0\}$ then there exists a nonzero element $a \in I$. But every nonzero element of a field is a unity, hence we have $I = R$ from part (a). Conversely, suppose R is a ring with only two ideals and consider any nonzero element $a \in R$. We will show that a is a unit. To do this, we consider the principal ideal aR. Since $a \neq 0$ we have $aR \neq \{0\}$, and it follows that $aR = R$. Then since $1 \in R$ we have $1 \in aR$, so that $1 = ab$ for some $b \in R$. In other words, a is a unit. Finally, since every nonzero element of R is a unit we conclude that R is a field.

(c): Let $I, J \subseteq R$ be ideals and consider their sum

$$I + J := \{a + b : a \in I, b \in J\}.$$

We will prove that $I + J \subseteq R$ is also an ideal. To do this, consider two elements $a + b$ and $a' + b'$ in $I + J$, with $a, a' \in I$ and $b, b' \in I$, and any element $c \in R$. Since I and J are ideals we have $a + ca' \in I$ and $b + cb' \in J$. But then we also have

$$(a + b) + c(a' + b') = (a + ca') + (b + cb') \in I + J.$$

Hence $I + J$ is an ideal. [Remark: This proof also shows that $I + J$ is an additive subgroup of R. If you are already willing to accept this fact then the proof can be made simpler.]

(d): For any elements $a_1, \ldots, a_n \in R$ we consider the set

$$a_1R + \cdots + a_nR := \{a_1r_1 + \cdots + a_nr_n : r_1, \ldots, r_n \in R\}.$$

Note that this is an ideal since for any $b \in R$ we have[1]

$$(a_1r_1 + \cdots + a_nr_n)b = a_1(r_1b) + \cdots + a_n(r_nb) \in a_1R + \cdots + a_nR.$$

And certainly this ideal contains each element a_i by taking $r_i = 1$ and $r_j = 0$ for $j \neq i$. Now let $I \subseteq R$ be an arbitrary ideal that contains the set $\{a_1, \ldots, a_n\}$. Then for any elements $r_1, \ldots, r_n \in R$ the ideal property tells us that

$$a_1r_1 + \cdots a_nr_n \in I,$$

and it follows that $a_1R + \cdots a_nR \subseteq I$.

[1]Here I don't bother to check that this set is an additive subgroup of R.

2. Prime and Maximal Ideals. Let $I \subseteq R$ be an ideal. We say that I is *maximal* when:

- $I \neq R$,
- There are no ideals of R between I and R.

We say that I is *prime* when for all $a, b \in R$ we have

$$ab \in I \quad \Longrightarrow \quad a \in I \text{ or } b \in I.$$

For any ideal $I \subseteq R$ recall that we have a *quotient ring* $(R/I, +, \cdot, [0], [1])$ with addition and multiplication defined by

$$[a] + [b] := [a + b] \quad \text{and} \quad [a][b] := [ab],$$

where $[a] = a + I$ denotes the additive coset generated by $a \in R$.

(a) Prove that R/I is a domain if and only if I is prime. [Hint: $[a] = [0] \Longleftrightarrow a \in I$.]
(b) Prove that R/I is a field if and only if I is maximal. [Hint: Use Problem 1.]
(c) Prove that every maximal ideal is prime.

(a): First uppose that I is a prime ideal. Then for any classes $[a], [b] \in R/I$ we have

$$\begin{aligned} [a][b] = [0] \quad &\Longrightarrow \quad [ab] = [0] \\ &\Longrightarrow \quad ab \in I \\ &\Longrightarrow \quad a \in I \text{ or } b \in I \\ &\Longrightarrow \quad [a] = [0] \text{ or } [b] = [0], \end{aligned}$$

and hence R/I is a domain. Conversely, suppose that R/I is a domain. Then for any elements $a, b \in R$ we have

$$\begin{aligned} ab \in I \quad &\Longrightarrow \quad [ab] = [0] \\ &\Longrightarrow \quad [a][b] = [0] \\ &\Longrightarrow \quad [a] = [0] \text{ or } [b] = [0] \\ &\Longrightarrow \quad a \in I \text{ or } b \in I, \end{aligned}$$

and hence I is a prime ideal.

(b): First suppose that I is a maximal ideal. In order to prove that R/I is a field, we will show that every nonzero class $[a] \neq [0]$ there exists some class $[b] \in R/I$ such that $[a][b] = [1]$. So consider any nonzero class $[a] \neq [0]$, i.e., any element $a \notin I$. Now consider the ideal $J = I + aR$. Since $a \notin I$ we have $I \subsetneq J$, which, since I is maximal, implies that $I + aR = R$. Then since $1 \in R$ we also have $1 \in aR + I$ and we can write $1 = ab + c$ for some $b \in R$ and $c \in I$. Finally, since $ab - 1 = c \in I$ we have

$$\begin{aligned} [ab] &= [1] \\ [a][b] &= [1], \end{aligned}$$

as desired. Conversely, suppose that R/I is a field. In order to prove that I is maximal, we will show that any ideal J satisfying $I \subsetneq J$ must satisfy $J = R$. So consider any ideal $I \subsetneq J$ and pick any element $a \in J \setminus I$. Since R/I is a field there exists $b \in R$ such that $[a][b] = [1]$, which implies that $ab - 1 \in I$. Since $I \subseteq J$ this implies that $ab - 1 = c$ for some c. Furthermore, since J is an ideal, we have

$$a \in J \text{ and } b \in R \quad \Longrightarrow \quad ab \in J.$$

We conclude that $1 = ab - c \in J$. But we know from 1(a) that any ideal containing a unit is the whole ring. Hence $J = R$, as desired.

Remark: This proof can be made much simpler if we accept the correspondence theorem for ideals, which for any ideal $I \subseteq R$ gives a bijection

$$\{\text{ideals } J \text{ of } R \text{ such that } I \subsetneq J \subsetneq R\} \leftrightarrow \{\text{ideals } J' \text{ of } R/I \text{ such that } \{[0]\} \subsetneq J' \subsetneq R/I\}.$$

From 1(b) we know that the right set is empty if and only if R/I is a field, and clearly the left set is empty if and only if I is a maximal ideal.

(c): Since every field is a domain, we have

$$\begin{aligned} I \text{ is maximal} &\implies R/I \text{ is a field} && 2(b) \\ &\implies R/I \text{ is a domain} \\ &\implies I \text{ is prime.} && 2(a) \end{aligned}$$

3. Divisibility in a Domain. Let R be an integral domain with group of units $R^\times$. Given $a, b \in R$ we define the relation of *divisibility*:

$$a|b \iff ac = b \text{ for some } c \in R.$$

And we define the relation of *association*:

$$a \sim b \iff au = b \text{ for some } u \in R^\times.$$

(a) Prove that $|$ is a partial order on R.
(b) For all $a, b \in R$ prove that $a|b$ if and only if $bR \subseteq aR$.
(c) Prove that $\sim$ is an equivalence relation on R.
(d) For all $a, b \in R$, prove that $a \sim b$ if and only if $aR = bR$.
(e) Sets of the form $aR \subseteq R$ are called *principal ideals* of R. Show that we have bijections:

$$\begin{aligned} \text{principal ideals of } \mathbb{Z} &\longleftrightarrow \mathbb{N}, \\ \text{principal ideals of } \mathbb{F}[x] &\longleftrightarrow \{0\} \cup \{\text{monic polynomials}\}. \end{aligned}$$

(A *monic polynomial* has leading coefficient 1.)

4. Quotient and Remainder of Polynomials. Consider the ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$. In this problem you will prove that for any polynomials $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, there exists a unique pair of polynomials $q(x), r(x) \in \mathbb{F}[x]$ — called the *quotient* and *remainder* of $f(x)$ modulo $g(x)$ — satisfying

$$\begin{cases} f(x) = g(x)q(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < \deg(g). \end{cases}$$

(a) **Existence.** Consider the set $S = \{f(x) - g(x)q(x) : q(x) \in \mathbb{F}[x]\} \subseteq \mathbb{F}[x]$. If $0 \in S$ then we are done, so suppose that $0 \notin S$. Let $r(x)$ be any element of S with minimal degree. In this case, prove that $\deg(r) < \deg(g)$. [Hint: Assume for contradiction that $\deg(r) \geq \deg(g)$. Let's say $g(x) = a_m x^m + \cdots$ and $r(x) = b_n x^n + \cdots$ with $m \leq n$. In this case, show that $h(x) := r(x) - \frac{b_n}{a_m} x^{n-m} g(x) \in S$ and $\deg(h) < \deg(r)$.]
(b) **Uniqueness.** Let $q(x), r(x)$ and $q'(x), r'(x)$ be two pairs satisfying the properties of quotient and remainder. In this case prove that $q(x) = q'(x)$ and $r(x) = r'(x)$. [Hint: By assumption we have $g(x)q(x) + r(x) = f(x) = g(x)q'(x) + r'(x)$, and hence $g(x)[q(x) - q'(x)] = r'(x) - r(x)$. If $r(x) = r'(x)$ then we are done, so suppose that $r(x) \neq r'(x)$. In this case, use properties of degree to show that $\deg(g) < \deg(r' - r)$ and derive a contradiction from this.]

(a): Given $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, consider the set

$$S = \{f(x) - g(x)q(x) : q(x) \in \mathbb{F}[x]\} \subseteq \mathbb{F}[x].$$

If $0 \in S$ then we have $f(x) = g(x)q(x)+0$ and we are done. Other wise, if $S \neq \{0\}$, let $r(x) \in S$ be any nonzero element of minimal degree. By definition of S we have $f(x) = g(x)q(x) + r(x)$ for some $q(x) \in \mathbb{F}[x]$. Hence it remains only to show that $\deg(r) < \deg(g)$. So suppose for contradiction that $\deg(g) \leq \deg(r)$. Let's say that $\deg(g) = m$ and $\deg(r) = n$ with $m \leq n$. Let's also name the coefficients:

$$\begin{aligned} g(x) &= a_m x^m + \cdots + a_1 x + a_0, \\ r(x) &= b_n x^n + \cdots + b_1 x + b_0. \end{aligned}$$

Since a_m is a nonzero element of a field $\mathbb{F}$ we may consider the polynomial

$$h(x) := r(x) - \frac{b_n}{a_m} x^{n-m} g(x) = (b_n - b_n)x^n + \text{ lower terms},$$

which has $\deg(h) < \deg(r)$. On the other hand, since $r(x) \in S$ we have $r(x) = f(x) - g(x)s(x)$ for some $s(x) \in \mathbb{F}[x]$ and hence

$$h(x) = f(x) - g(x)s(x) - \frac{b_n}{a_m} x^{n-m} g(x) = f(x) - \left(s(x) + \frac{b_n}{a_m} x^{n-m} \right) g(x) \in S.$$

Thus $h(x)$ is a nonzero element of S with degree strictly less than $\deg(r)$. Contradiction.

(b): Consider any $f(x), g(x) \in \mathbb{F}[x]$ with $g(x)$, and consider any polynomials $q(x), r(x), q'(x), r'(x) \in \mathbb{F}[x]$ satisfying

$$\begin{cases} f(x) = g(x)q(x) + r(x), \\ r(x) = 0 \text{ or } \deg(r) < \deg(g), \end{cases} \qquad \begin{cases} f(x) = g(x)q'(x) + r'(x), \\ r'(x) = 0 \text{ or } \deg(r') < \deg(g). \end{cases}$$

Since $g(x)q(x) + r(x) = f(x) = g(x)q'(x) + r'(x)$ we have $g(x)[q(x) - q'(x)] = [r'(x) - r(x)]$. If $r(x) = r'(x)$ then we have $g(x)[q(x) - q'(x)] = 0$. Since $g(x) \neq 0$ this implies that $q(x) - q'(x) = 0$ and hence $q(x) = q'(x)$ as desired. So let us suppose for contradiction that $r'(x) - r(x)$. Since $g(x) \neq 0$ this also implies that $q(x) - q'(x)$. Then applying degrees to the equation $g(x)[q(x) - q'(x)] = [r'(x) - r(x)]$ gives a contradiction:

$$\deg(g) \leq \deg(g) + \deg(q - q') = \deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g).$$

5. Euclidean Rings Have Only Principal Ideals. A ring R is called *Euclidean* if there exists a "size function"[2] $N : R \setminus \{0\} \to \mathbb{N}$ that satisfies the "Euclidean algorithm": For all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$\begin{cases} a = bq + r, \\ r = 0 \text{ or } N(r) < N(b). \end{cases}$$

If R is a Euclidean ring, prove that every ideal of R has the form aR for some $a \in R$. [Hint: Consider any ideal $I \subseteq R$. If $I = \{0\}$ then we are done, so suppose $I \neq \{0\}$ and let $a \in I$ be any nonzero element of minimal "size" $N(a)$. Prove that $I = aR$.]

Proof. Let (R, N) be a Euclidean ring and consider any ideal $I \subseteq R$. If $I = \{0\}$ then we have $I = 0R$ and we are done. So suppose that $I \neq \{0\}$ and let $a \in I$ be any nonzero element of

[2]There are two main examples of size functions: absolute value of integers and degree of polynomials. However, these examples have some peculiar features that make it difficult to set up a satisfying general theory of size functions. For this reason, Euclidean rings are usually thrown away in favor of *principal ideal rings*, even though these two concepts are not identical. Principal ideal rings (PIRs) and principal ideal domains (PIDs) lead to a more satisfying general theory.

minimal size $N(a)$ (which exists because $\mathbb{N}$ well-ordered). In this case I claim that $I = aR$. Indeed, since I is an ideal of R that contains a we must have $aR \subseteq I$ as in Problem 1(d). Conversely, we will show that any element $b \in I$ has the form $b = aq$ for some $q \in R$, and hence $I \subseteq aR$. So let b be any element of I and divide by the nonzero element $a \in R$ to obtain

$$\begin{cases} b = aq + r, \\ r = 0 \text{ or } N(r) < N(a). \end{cases}$$

If $r \neq 0$ then we have $N(r) < N(a)$ and $r = a - bq \in I$ so that r is a nonzero element of I with size strictly less than $N(a)$, which is a contradiction. Hence we must have $r = 0$ and hence $b = aq \in aR$. We have shown that $aR \subseteq I$ and $I \subseteq aR$, hence $I = aR$.

6. The Ring $\mathbb{Z}[x]$ is Not Euclidean. Prove indirectly that $\mathbb{Z}[x]$ is not Euclidean by showing that the following ideal is not principal:

$$\begin{aligned} 2\mathbb{Z}[x] + x\mathbb{Z}[x] &= \{2f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\} \\ &= \{\text{integer polynomials whose constant term is even}\}. \end{aligned}$$

[Hint: Suppose for contradiction that $I = c(x)\mathbb{Z}[x] = \{c(x)f(x) : f(x) \in \mathbb{Z}[x]\}$ for some polynomial $c(x) \in \mathbb{Z}[x]$. If $\deg(c) \geq 1$ then every nonzero element of I has degree ≥ 1. But $2 \in I$. Hence $c(x) = c \in \mathbb{Z}$ is a nonzero integer. If $c = \pm 1$ then we also have $\pm 1 \in I$, which contradicts the fact that every polynomial in I has even constant term. If $|c| \geq 2$ then every polynomial in I has coefficients of absolute value ≥ 2, contradicting the fact that $x \in I$.]

Proof. Suppose for contradiction that $I = c(x)\mathbb{Z}[x]$ for some $c(x) \in \mathbb{Z}[x]$. Since $I \neq \{0\}$ we must have $c(x) \neq 0$. If $\deg(c) \geq 1$ then every nonzero element $f(x) \in c(x)\mathbb{Z}[x]$ has the form $f(x) = c(x)g(x)$ for some nonzero $g(x)$ and hence $\deg(f) = \deg(c) + \deg(g) \geq \deg(c) \geq 1$. But $2 \in I$ and $\deg(2) < 1$. We have shown that $c(x) = c \in \mathbb{Z}$ is a nonzero integer. I claim that $c = \pm 1$. If not then we must have $|c| \geq 2$. But any element of $I = c\mathbb{Z}[x]$ can be expressed as $c(\sum_k a_k x^k)$, with coeffiients $ca_k \in \mathbb{Z}$. If $ca_k \neq 0$ then $a_k \neq 0$ and hence $|a_k| \geq 1$. But then

$$|ca_k| = |c||a_k| \geq 2 \cdot 1 = 2,$$

which shows that the nonzero coefficients of polynomials in I have absolute value ≥ 2. This contradicts the fact that $x \in I$. At this point we have shown that $I = \pm\mathbb{Z}[x] = \mathbb{Z}[x]$. But, finally, this contradicts the fact that $1 \notin I$.

Remark: A similar proof shows that the ideal $x\mathbb{F}[x, y] + y\mathbb{F}[x, y] \subseteq \mathbb{F}[x, y]$ is not principal, and hence the ring of polynomials $\mathbb{F}[x, y]$ in two variables over a field $\mathbb{F}$ is not Euclidean. However, it is **extremely difficult** to describe all of the ideals in the ring of polynomials $\mathbb{F}[x_1, \ldots, x_n]$ in many variables. (It is even difficult to prove that every ideal is finitely generated. This is the famous Hilbert Basis Theorem.) Euclidean domains are really special.