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 $\{a_1, \ldots, a_n\}$.

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.

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*:

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

And we define the relation of *association*:

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

(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:

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

(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.]

5. Euclidean Rings Have Only Principal Ideals. A ring R is called *Euclidean* if there exists a "size function"[1] $N : R \setminus \{0\} \to \mathbb{N}$ 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 $I = aR$.]

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 $x \in I$.]

[1] 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.