Math 561/661 **Fall 2021**
Homework 3 **Drew Armstrong**

---

1. Units and Associates. We say that $u \in R$ is a *unit* if there exists $v \in R$ with $uv = 1$. Let $R^\times$ be the set of units. We say that $a, b \in R$ are *associates* if there exists a unit $u \in R^\times$ such that $au = v$. We define the notation

$$a \sim b \quad \Longleftrightarrow \quad \exists u \in R^\times, au = b.$$

(a) Prove that $\sim$ is an equivalence relation on the set R.
(b) Prove that $\mathbb{Z}^\times = \{\pm 1\}$. [Hint: Use absolute value.]
(c) Prove that $\mathbb{F}[x]^\times = \mathbb{F} \setminus \{0\}$. [Hint: Use degree.]

2. Lemmas for the Euclidean Algorithm.

(a) For elements a, b, c, x in a ring R satisfying $a = bx + c$, prove that the following sets of common divisors are equal:

$$\text{Div}(a, b) = \text{Div}(b, c).$$

[Hint: You need to prove the inclusion in both directions.]

(b) Now let R be a Euclidean domain with size function $N : R \setminus \{0\} \to \mathbb{N}$. For any nonzero element $a \in R$, prove that

$$d \sim a \quad \Longleftrightarrow \quad d \text{ is a maximum-sized element of } \text{Div}(a).$$

[Hint: Every divisor $d|a$ satisfies $N(d) \leq N(a)$, so a itself is among the maximum-sized divisors of a. Use this to show that every associate of a is a maximum-sized divisor. Conversely, let $d|a$ be a maximum-sized divisor, i.e., with $N(d) = N(a)$. To prove $d \sim a$ you need to show $a|d$. Divide d by a and show that the remainder r is divisible by d. Then show that $r \neq 0$ leads to a contradiction.]

3. Roots are Irrational. Let $d \geq 1$ be a positive integer and let $\sqrt[n]{d} > 0$ be its unique positive nth root. We will prove the following:

$$\text{If } \sqrt[n]{d} \text{ is not an integer then } \sqrt[n]{d} \text{ is not a rational number.}$$

In the proof we will use the notation $\nu_p(a)$ for the *multiplicity* of the prime p in the unique prime factorization of the integer a.

(a) Show that $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ for all primes p and integers $a, b \in \mathbb{Z}$.
(b) Given $a, n \in \mathbb{Z}$, show that $n|\nu_p(a^n)$ for all primes p. If $d \in \mathbb{Z}$ is not the nth power of an integer then it follows that there exists a prime p with $n \nmid \nu_p(d)$.
(c) If $d \in \mathbb{Z}$ is not the nth power of an integer, prove that it is not the nth power of a rational number. [Hint: Assume for contradiction that $d = (a/b)^n$. Multiply both sides by b^n. Then use parts (a) and (b).]

4. Modular Arithmetic. Fix a positive integer $n \geq 1$. Following Gauss, we define the following notation for all $a, b \in \mathbb{Z}$, and we call this *congruence modulo* n:

$$a \equiv b \mod n \quad \Longleftrightarrow \quad n|(a - b).$$

(a) Prove that congruence mod n is an equivalence relation on the set $\mathbb{Z}$.
(b) Prove that congruence mod n respects addition and multiplication. In other words, if $a \equiv a'$ and $b \equiv b'$ mod n, prove that $a + b \equiv a' + b'$ and $ab \equiv a'b'$ mod n. [Hint: For the second property, consider the identity $ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'$.]

(c) Prove that for all $a \in \mathbb{Z}$ there exists a unique integer $r \in \mathbb{Z}$ satisfying $a \equiv r \bmod n$ and $0 \leq r \leq n-1$. [Hint: Let r be the remainder of a when divided by n. Suppose that $a \equiv r$ and $a \equiv r' \bmod n$ for some $0 \leq r, r' \leq n-1$. If $r \neq r'$ then it follows that $n|(r-r')$ and hence $|n| \leq |r-r'|$. Use this to obtain a contradiction.]

It follows that the finite set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ can be viewed as a ring.[1]

5. Some Finite Fields. In class we proved that for all $a, b, p \in \mathbb{Z}$ with p prime we have

$$p|ab \quad \Longrightarrow \quad p|a \text{ or } p|b.$$

(a) If p is prime, use this property to prove that $\mathbb{Z}/p\mathbb{Z}$ is an integral domain. Since this set is finite, it follows from the previous homework that $\mathbb{Z}/p\mathbb{Z}$ is a field.

(b) Since 23 is prime it follows from part (a) that the nonzero element $16 \in \mathbb{Z}/23\mathbb{Z}$ has a multiplicative inverse. Use the Vector Euclidean Algorithm to find this element. [Hint: Find some $x, y \in \mathbb{Z}$ such that $23x + 16y = 1$.]

(c) If $n \geq 1$ is not prime, prove that $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain.

[1] I will explain the notation $\mathbb{Z}/n\mathbb{Z}$ later.