Math 461 **Spring 2023**
Homework 2 **Drew Armstrong**

---

1. The Group of Units. Let R be any commutative ring, and consider the set of *units*

$$R^\times = \{u \in R : \text{ there exists } v \in R \text{ such that } uv = 1\}.$$

(a) Prove that $1 \in R$ is a unit and $0 \in R$ is not a unit.
(b) The definition of $u \in R^\times$ says that u has at least one multiplicative inverse. Prove that this multiplicative inverse must be unique. We will call it u^{-1}.
(c) If u is a unit, prove that u^{-1} is also a unit.
(d) If u and v are units, prove that uv is also a unit.

Remark: These properties tell us that $(R^\times, \cdot, 1)$ is a *group*.

2. Associatedness. Let R be any commutative ring and let $R^\times$ be the group of units. For any $a, b \in R$ we define the relation of *associatedness*:[1]

$$a \sim b \quad \iff \quad \text{there exists a unit } u \in R^\times \text{ such that } au = b.$$

In this case we say that a and b are *associates.*

(a) Prove that $a \sim 1$ if and only if $a \in R^\times$, and $a \sim 0$ if and only if $a = 0$.
(b) For any $a \in R$ prove that $a \sim a$.
(c) For any $a, b \in R$ prove that $a \sim b$ if and only if $b \sim a$.
(d) For any $a, b, c \in R$ prove that $a \sim b$ and $b \sim c$ imply $a \sim c$.

Hint: Quote Problem 1 when necessary.

3. Partial Fractions. Let R be a domain and let $a, b \in R$ be coprime. This means that

$$aR + bR = R.$$

(a) Prove that there exist $x, y \in R$ satisfying $ax + by = 1$.
(b) Using part (a), prove that there exist $A, B \in R$ satisfying

$$\frac{1}{ab} = \frac{A}{a} + \frac{B}{b}.$$

Remark: The elements A, B are not unique.
(c) Compute some A, B for $a = 13$ and $b = 21$ in $R = \mathbb{Z}$.
(d) Compute some A, B for $a = x + 1$ and $b = x^2 + 1$ in $R = \mathbb{R}[x]$.

Remark: These examples are small enough that you can use ad hoc methods. For larger examples, one would use the Extended Euclidean Algorithm, as in Problem 5.

4. Greatest Common Divisor. Let $a, b \in R$ be elements of a commutative ring. We say that $c \in R$ is a *greatest common divisor* (gcd) of a and b when

$$aR + bR = cR.$$

(a) Let c be a gcd of a and b. In this case prove that $c|a$ and $c|b$. [Remark: This is the sense in which a greatest common divisor is a "common divisor".]
(b) Let c be a gcd of a and b and let d be any common divisor of a and b (i.e., suppose that $d|a$ and $d|b$). In this case, prove that $d|c$. [Remark: This is the sense in which a greatest common divisor is "greatest".]
(c) Greatest common divisors need not be unique. However, if R is a domain prove that any two greatest common divisors of a and b are associates.

---

[1] Remark: This awkward notation has no connection with "associativity" of binary operators.

Remark: Greatest common divisors need not exist. However, if R is a Euclidean domain then we proved in class that they do exist.

5. The Euclidean Algorithm.

(a) *Missing Lemma.* Let R be a commutative ring and suppose that we have $a = bx + c$ for some elements $a, b, c, x \in R$. In this case prove that

$$aR + bR = bR + cR.$$

It follows that the pairs (a, b) and (b, c) have the same common divisors.

(b) Use the Extended Euclidean Algorithm (as described in class and the notes) to find some integers $x, y \in \mathbb{Z}$ satisfying

$$32x + 47y = 1.$$

6. Fermat Primes. Let $k \geq 1$ and assume that the number $2^k + 1$ is prime. In this case we will show that k must be a power of 2.

(a) If $k = \ell m$ with m **odd**, show that $2^k + 1$ is divisible by $2^\ell + 1$. [Hint: We know from Homework 1 that $a^m - b^m$ is divisible by $a - b$ for any integers a, b, m with $m \geq 1$. Substitute appropriate values for a and b.]

(b) If k is not a power of 2, use part (a) to show that $2^k + 1$ is not prime. [Hint: If k is not a power of 2 then it has an **odd** prime divisor, say $p|k$.]