Math 562 | **Spring 2014**
Homework 1 | **Drew Armstrong**

Problems on Integers

1. The Division Algorithm. Consider integers $a, b \in \mathbb{Z}$ with $b \neq 0$.

(a) Prove that there exist integers $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$. [Hint: Let S be the set of integers of the form $a - qb$ for some $q \in \mathbb{Z}$. By well ordering, the set S has a smallest nonnegative element which we can call r. Show that r is small enough.]

(b) Prove that the integers q, r from part (a) are unique. [Hint: Suppose that $a = q_1 b + r_1 = q_2 b + r_2$ with $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$. Show that the assumption $r_1 - r_2 \neq 0$ leads to a contradiction.]

(c) Use the Division Algorithm to prove that the equation $2x = 1$ has no solution $x \in \mathbb{Z}$.

Proof. Consider integers $a, b \in \mathbb{Z}$ with $b \neq 0$. For part (a), define the set

$$S := \{a - qb : q \in \mathbb{Z}\}.$$

By well ordering, the set S has a smallest nonnegative element. Call it $r \geq 0$. Then by definition of S there exists $q \in \mathbb{Z}$ such that $a = qb + r$. I claim that $0 \leq r < |b|$. Suppose not, i.e., suppose that we have $|b| \leq r$. In this case we have $0 \leq r - |b| < |b|$. But we also have

$$r - |b| = a - qb - |b| = a - (q \pm 1)b \in S,$$

which contradicts the fact that r is the smallest nonnegative element of S. We have proven that there exist $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < |b|$ as desired.

For part (b), suppose that there exist $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$q_1 b + r_1 = a = q_2 b + r_2$$

with $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$. We want to show that $q_1 = q_2$ and $r_1 = r_2$. Suppose not, i.e., suppose that $r_1 \neq r_2$, say $r_1 < r_2$. Then we have

$$0 < (r_2 - r_1) \leq r_2 < |b|.$$

But we also have

$$\begin{aligned} q_1 b + r_1 &= q_2 b + r_2, \\ q_1 b - q_2 b &= r_2 - r_1, \\ (q_1 - q_2) b &= (r_2 - r_1). \end{aligned}$$

Since $r_2 - r_1 \neq 0$ we have $q_1 - q_2 \neq 0$ which implies that $1 \leq |q_1 - q_2|$, hence

$$|b| \leq |q_1 - q_2||b| = |(q_1 - q_2)b| = |r_2 - r_1| \leq (r_2 - r_1).$$

Contradiction. We conclude that $r_1 = r_2$. Then since $(q_1 - q_2)b = 0$ and $b \neq 0$ we conclude that $(q_1 - q_2) = 0$, hence $q_1 = q_2$. [Interesting question: **Why** is $\mathbb{Z}$ a domain?]

For part (c), assume for contradiction that there exists $x \in \mathbb{Z}$ such that $2x = 1$. Since

$$1 = 2x + 0 \quad \text{with} \quad 0 \leq 0 < 2$$

we see that 0 is the remainder when 1 is divided by 2. But we also have

$$1 = 2 \cdot 0 + 1 \quad \text{with} \quad 0 \leq 1 < 2$$

so 1 is the remainder when 1 is divided by 2. This contradicts the uniqueness of remainder proved in part (b). □

[Now we can confidently say that $1/2$ is not an integer; that is, after we explain why $\mathbb{Z}$ is a domain.]

2. Application of Unique Factorization.

(a) Consider $a, p \in \mathbb{Z}$ with p prime and $a \neq 0$. Prove that p occurs an even number of times in the prime factorization of a^2.

(b) Use part (a) to give a short proof that $\sqrt{2}$ is irrational. [Hint: Assume for contradiction that there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ and $a/b = \sqrt{2}$.]

Proof. For part (a), suppose that $a \in \mathbb{Z}$ can be written as a product

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1 < p_2 < \cdots < p_k$ are distinct primes. Then we have

$$a^2 = (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k},$$

thus any given prime occurs an even number of times in the prime factorization of a^2 (zero is a perfectly good number of times).

For part (b), assume for contradiction that there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ and $a/b = \sqrt{2}$. Then we have

$$\begin{aligned} a/b &= \sqrt{2}, \\ a &= b\sqrt{2}, \\ a^2 &= 2b^2. \end{aligned}$$

But the prime 2 occurs an even number of times in a^2 and an odd number of times in $2b^2$. This contradicts the uniqueness of prime factorization. $\square$

[You can use the same method to prove that $\sqrt{d}$ is irrational for any $d \in \mathbb{Z}$ such that $\sqrt{d} \notin \mathbb{Z}$.]

Problems on Rings

3. Properties of subtraction.

(a) Given $a \in R$ the axioms say that there exists $a' \in R$ such that $a + a' = 0$. Prove that this a' is unique. We will call it $-a$. Then we define the operation of **subtraction** by

$$a - b := a + (-b).$$

(b) Prove that $a0 = 0$ for all $a \in R$.

(c) Prove that for all $a, b \in R$ we have $(-a)b = -(ab)$. [Hint: Use part (b).]

(d) Prove that for all $a, b \in R$ we have $(-a)(-b) = ab$. [Hint: Use part (c) to show that $ab + a(-b) = 0$. Then use (b).] If a child asks you **why** negative times negative is positive, now you will know what to say.

(e) Prove that for all $a, b, c \in R$ we have $a(b - c) = ab - ac$. [Hint: Use part (c).]

Proof. For part (a), suppose we have a' and a'' in R such that

$$a + a' = 0 = a + a''.$$

It follows that

$$a' = a' + 0 = a' + (a + a'') = (a' + a) + a'' = 0 + a'' = a''.$$

We will write $-a := a' = a''$ for the unique additive inverse.

For part (b) first note that

$$a0 = a(0 + 0) = a0 + a0.$$

Then add $-0a$ to both sides to conclude that $0 = a0$.

For part (c) we want to show that $(-a)b$ is the additive inverse of ab. Indeed, using the result of part (a) we have

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

For part (d) first note that $a(-b) = -(ab)$. This follows from part (c) and commutativity. Then apply part (c) again to get

$$ab = -(a(-b)) = (-a)(-b).$$

Finally, for part (e) we apply part (c) again to get

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac.$$

□

4. Let $\varphi : R \to S$ be a ring homomorphism.

(a) Prove that $\varphi(0_R) = 0_S$.
(b) Prove that $\varphi(-a) = -\varphi(a)$ for all $a \in R$.
(c) Let $a \in R$. If a^{-1} exists, prove that $\varphi(a)$ is invertible with $\varphi(a)^{-1} = \varphi(a^{-1})$.

Proof. Let $\varphi : R \to S$ be a ring homomorphism. That is, we have $\varphi(1_R) = 1_S$ and for all $a, b \in R$ we have $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$. To prove part (a) note that

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R).$$

Now subtract $\varphi(0_R)$ from both sides to get $0_S = \varphi(0_R)$. For part (b), let $a \in R$. Then using part (a) we have

$$0_S = \varphi(0_R) = \varphi(a - a) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a).$$

Now subtract $\varphi(a)$ from both sides to get $-\varphi(a) = \varphi(-a)$.

For part (c), let $a \in R$ and suppose that there exists $a^{-1} \in R$ with $aa^{-1} = 1_R$. Applying φ to this equation gives

$$1_S = \varphi(1_R) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}).$$

We conclude that $\varphi(a)^{-1} = \varphi(a^{-1})$. □

[Note that we needed to assume $\varphi(1_R) = 1_S$ in the definition of ring homomorphism. It does not follow automatically from the fact that $\varphi(ab) = \varphi(a)\varphi(b)$. We might try to say that

$$\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$$

and then cancel $\varphi(1_R)$ from both sides to get $1_S = \varphi(1_R)$. But this doesn't work because $(R, \times, 1)$ is just a semigroup, not a group.]

5. Let R be a ring. We say that $a \in R$ is nilpotent if $a^n = 0$ for some n. If a is nilpotent, prove that $1 + a$ and $1 - a$ are units (i.e. invertible).

Proof. Note that for all $a \in R$ and $n \in \mathbb{N}$ we have the identities:

$$1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1}),$$
$$1 - (-1)^n a^n = (1 + a)(1 - a + a^2 - \cdots + (-1)^{n-1} a^{n-1}).$$

If $a^n = 0$ then we obtain inverses for $1 + a$ and $1 - a$. □

6. Let $I \leq R$ be an ideal. Prove that $I = R$ if and only if I contains a unit.

Proof. If $I = R$ then we have $1 \in I$ and so I contains a unit. Conversely, suppose that we have $u \in I$ and that there exists $u^{-1} \in R$. Since I is an ideal this implies that $1 = uu^{-1} \in I$ and then for all $a \in R$ we have $a = 1a \in I$. Hence $I = R$. □

[For this reason, $R = (1)$ is sometimes called the "unit ideal".]

7. Given an ideal $I \leq R$ and an element $a \in R$ we define the additive coset

$$a + I := \{a + x : x \in I\}.$$

Now consider $a, a', b, b' \in R$ such that $a + I = a' + I$ and $b + I = b' + I$. Prove that $(a+b)+I = (a'+b')+I$ and $(ab)+I = (a'b')+I$. This shows that addition and multiplication of cosets is well-defined.

Proof. We assume that $a + I = a' + I$ and $b + I = b' + I$; that is, there exist $x, y \in I$ such that $a - a' = x$ and $b - b' = y$. First we show that $(a + b) + I = (a' + b') + I$. Indeed, we have

$$\begin{aligned}(a + b) &= (a' + x) + (b' + y), \\ &= (a' + b') + (x + y).\end{aligned}$$

Since $x + y \in I$ we conclude that $(a + b) - (a' + b') \in I$ as desired. Next we show that $(ab) + I = (a'b') + I$. Indeed, we have

$$\begin{aligned}(ab) &= (a' + x)(b' + y), \\ &= (a'b') + (a'y + xb' + xy).\end{aligned}$$

Since $a'y + xb' + xy \in I$ we conclude that $(ab) - (a'b') \in I$ as desired. □

[We have proved that the set R/I has well-defined addition and multiplication. One can then show that these operations define a ring structure on R/I. It seems that every book on the subject leaves out this verification as too "boring". I will not disagree.]