Math 461 **Exam 1**
Spring 2023 **Thurs Feb 23**

No electronic devices are allowed. There are 5 pages and each page is worth 6 points, for a total of 30 points.

Problem 1. Units. Let R be a (commutative) ring. An element $u \in R$ is called a *unit* when there exists an element $r \in R$ such that $ur = 1$.

(a) If $ur_1 = 1$ and $ur_2 = 1$, prove that $r_1 = r_2$. Hence the inverse of of u (if it exists) is unique. We typically call it u^{-1}.

Proof. If $ur_1 = 1$ and $ur_2 = 1$ then we have

$$r_1 = 1r_1 = (ur_2)r_1 = (ur_1)r_2 = 1r_2 = r_2.$$

(b) If u and v are units, prove that the product uv is also a unit.

Proof. Let u and v be units. By definition this means that $ur = 1$ and $vr' = 1$ for some elements $r, r' \in R$. But then

$$1 = 1 \cdot 1 = (ur)(vr') = (uv)(rr') = (uv)(\text{some element of } R),$$

which tells us that uv is a unit.

Remark: If we incorporate part (a) then we can say that $(uv)^{-1} = u^{-1}v^{-1}$.

Problem 2. Domains. Let R be a (commutative) ring. We say that R is a *domain* (also called an *integral domain*) if for all $a, b \in R$ we have

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ or } b = 0.$$

(a) Assuming that R is a domain, prove that $ab = ac$ and $a \neq 0$ imply $b = c$.

Proof. Let a, b, c be elements of a domain R satisfying $ab = ac$ and $a \neq 0$. Then

$$\begin{aligned} ab &= ac \\ ab - ac &= 0 \\ a(b - c) &= 0 \\ b - c &= 0 && \text{because } a \neq 0 \text{ and } R \text{ is a domain} \\ b &= c. \end{aligned}$$

(b) A *field* is a (commutative) ring in which every nonzero element is a unit. Prove that every field is a domain.

Proof. Let $\mathbb{F}$ be a field. Our goal is to show for all $a, b \in \mathbb{F}$ that $ab = 0$ implies $a = 0$ or $b = 0$. Equivalently, we will show that $ab = 0$ and $a \neq 0$ imply $b = 0$.

So suppose that $ab = 0$ and $a \neq 0$. Since $a \neq 0$ and $\mathbb{F}$ is a field, the multiplicative inverse a^{-1} exists. Now multiply both sides of $ab = 0$ by a^{-1} to get

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= a^{-1}0 \\ b &= 0. \end{aligned}$$

Problem 3. Divisibility. Let R be a (commutative) ring.

(a) Given elements $a, b \in R$, state the definition of the symbol "$a|b$".

$$\text{"}a|b\text{"} \quad \Longleftrightarrow \quad \text{"there exists an element } k \in R \text{ such that } ak = b\text{"}.$$

(b) Given an element $a \in R$ we define the set $aR = \{ar : r \in R\}$. If $bR \subseteq aR$, prove that $a|b$. [Hint: First show that $b \in bR$.]

Proof. Suppose that $bR \subseteq aR$. Since $b = b1$ and $1 \in R$ we see that $b \in bR$. Then since $bR \subseteq aR$ we see that $b \in aR$. By definition of aR this means that $b = ar$ for some $r \in R$, and hence $a|b$ as desired.

(c) Conversely, if $a|b$, prove that $bR \subseteq aR$.

Proof. Suppose that $a|b$, so that $ak = b$ for some $k \in R$. In order to show that $bR \subseteq aR$ we must show that every element of bR is an element of aR. So consider an arbitrary element $br \in bR$. Then we have

$$br = (ak)r = a(kr) = a(\text{some element of } R) \in aR,$$

as desired.

Problem 4. Greatest Comomon Divisors.

(a) Use the Extended Euclidean Algorithm to find some specific integers $x, y \in \mathbb{Z}$ satisfying $32x + 14y = 2$. [There are infinitely many correct answers.]

Consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ satisfying $32x + 14y = z$. Starting with the obvious triples $(1, 0, 32)$ and $(0, 1, 14)$, we perform row operations to obtain a triple of the form $(x, y, 2)$:

x	y	z
1	0	32
0	1	14
1	-2	4
-3	7	2

The final row tells us that $32(-3) + 14(7) = 2$. [Remark: In this case it is not possible to find $x, y \in \mathbb{Z}$ satisfying $32x + 14y = 1$ because 32 and 14 not coprime.]

(b) For any integers $a, b \in \mathbb{Z}$ we define the set $a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}$. Use your result from part (a) to prove that $32\mathbb{Z} + 14\mathbb{Z} = 2\mathbb{Z}$. [Hint: You need to show that $32\mathbb{Z} + 14\mathbb{Z} \subseteq 2\mathbb{Z}$ and $2\mathbb{Z} \subseteq 32\mathbb{Z} + 14\mathbb{Z}$.]

Proof. First we show that $32\mathbb{Z} + 14\mathbb{Z}$ is a subset of $2\mathbb{Z}$. To do this, consider an arbitrary element $32x + 14y \in 32\mathbb{Z} + 14\mathbb{Z}$. Then we have

$$32x + 14y = (2 \cdot 16)x + (2 \cdot 7)y = 2(16x + 7y) \in 2\mathbb{Z},$$

as desired. Conversely, we will show that $2\mathbb{Z}$ is a subset of $32\mathbb{Z} + 14\mathbb{Z}$. To do this, consider an arbitrary element $2z \in 2\mathbb{Z}$. Then from part (a) we have

$$2z = (32(-3) + 14(7))z = 32(-3z) + 14(7z) \in 32\mathbb{Z} + 14\mathbb{Z},$$

as desired.

Problem 5. Descartes' Theorem. Consider ring of polynomials $\mathbb{F}[x]$ over a field $\mathbb{F}$.

(a) Consider a polynomial $f(x) \in \mathbb{F}[x]$ and a constant $a \in \mathbb{F}$ satisfying $f(a) = 0$. Prove that $f(x) = (x - a)g(x)$ for some polynomial $g(x)$. [Hint: Consider the quotient and remainder when $f(x)$ is divided by $x - a$.]

Proof. Dividing $f(x)$ by $x - a$ in the ring $\mathbb{F}[x]$ gives (unique) polynomials $q(x), r(x) \in \mathbb{F}[x]$ satisfying

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

Since $\deg(x - a) = 1$, the second condition says that $r(x) = c$ for some constant $c \in \mathbb{F}$. To determine this constant we substitute $x = a$ to get

$$f(a) = (a - a)q(a) + c = 0q(a) + c = c.$$

It follows that $f(x) = (x - a)q(x) + f(a)$ for some polynomial $q(x)$. And if $f(a) = 0$ then we get $f(x) = (x - a)q(x)$ as desired.

(b) In part (a) you showed that $f(x) = (x - a)g(x)$ for some polynomial $g(x)$. Now suppose that $f(b) = 0$ for some other constant $b \neq a$. In this case show that $f(x) = (x - a)(x - b)h(x)$ for some polynomial $h(x)$. [Hint: Show that $g(b) = 0$.]

Proof. Suppose that $f(a) = 0$. In part (a) we showed that $f(x) = (x - a)g(x)$ for some polynomial $g(x)$. Now suppose that $f(b) = 0$ for some other constant $b \neq a$. Substituting $x = b$ gives

$$\begin{aligned} f(b) &= (b - a)g(b) \\ 0 &= (b - a)g(b). \end{aligned}$$

Since $\mathbb{F}$ is a domain (indeed, every field is a domain) and $b - a \neq 0$ this implies that $g(b) = 0$. Then by applying (a) we must have $g(x) = (x - b)h(x)$ for some polynomial $h(x)$, and hence

$$f(x) = (x - a)g(x) = (x - a)(x - b)h(x).$$