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*.

(a): If $v = 1$ then $1v = 1$, so 1 is a unit. To prove that 0 is not a unit, assume for contradiction that $0v = 1$ for some $v \in R$. Then then since $0v = 0$ we have $0 = 1$. Contradiction.

(b): Suppose that $uv = 1$ and $uw = 1$. Then we have

$$v = 1v = (uw)v = (uv)w = 1w = w.$$

(c): Take $v = u$. Then the equation $u^{-1}v = 1$ says that u^{-1} is a unit.

(d): Suppose that u and v are units so that u^{-1} and v^{-1} exist. Then since

$$(uv)(u^{-1}v^{-1}) = (uu^{-1})(vv^{-1}) = 1 \cdot 1 = 1,$$

we conclude that uv is a unit. In particular, we have $(uv)^{-1} = u^{-1}v^{-1}$.[1]

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*:[2]

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

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.

(a): Suppose that $a \sim 1$. By definition this means that $au = 1$ for some unit $u \in R^\times$. Then taking $v = u$ shows that $av = 1$ for some $v \in R$. Hence a is a unit. Conversely, let a be a unit so that $av = 1$ for some $v \in R$. Then Problem 1(b,c) implies that v is a unit, hence $a \sim 1$.

If $a = 0$ then $au = 0$ for **any** unit u, hence $a \sim 0$. Conversely, suppose that $a \sim 0$ so that $au = 0$ for some unit u. Since u^{-1} exists this implies that

$$\begin{aligned} au &= 0 \\ auu^{-1} &= 0u^{-1} \\ a &= 0. \end{aligned}$$

---

[1] In **non-commutative rings** we must take $(uv)^{-1} = v^{-1}u^{-1}$ instead of $u^{-1}v^{-1}$. For example, in the theory of matrix multiplication.

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

(b): For any a we have $a1 = a$. Since 1 is a unit (Problem 1a) this implies that $a \sim a$.

(c): Suppose that $a \sim b$, which means that $au = b$ for some unit u. Since u^{-1} exists, we have

$$\begin{aligned} au &= b \\ a &= bu^{-1}. \end{aligned}$$

Then since u^{-1} is a unit (Problem 1c) we have $b \sim a$. The other direction follows from switching the roles of a and b.

(d): Suppose $a \sim b$ and $b \sim c$ so that $au = b$ and $bv = c$ for some units u and v. Then we have

$$c = bv = (au)v = a(uv),$$

and since uv is a unit (Problem 1d) this implies that $a \sim c$.

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.

(a): Assume that $aR + bR = R$. Then since $1 \in R$ we have $1 \in aR + bR$, which by definition says that $1 = ax + by$ for some $x, y \in R$.

(b): From part (a) we have $1 = ax + by$ for some $x, y \in R$. Divide both sides by ab to get

$$\frac{1}{ab} = \frac{ax + by}{ab} = \frac{by}{ab} + \frac{ax}{ab} = \frac{y}{a} + \frac{x}{b}.$$

Thus we can take $A = y$ and $B = x$.

(c): We will use the Extended Euclidean Algorithm to find $x, y \in \mathbb{Z}$ such that $13x + 21y = 1$. To do this we consider all triples $(x, y, z) \in \mathbb{Z}^3$ such that $13x + 21y = z$. Starting with the easy triples $(0, 1, 21)$ and $(1, 0, 13)$, we perform row operations to obtain a triple of the form $(x, y, 1)$:

x	y	z	operation
0	1	21	(row 1)
1	0	13	(row 2)
-1	1	8	(row 3) = (row 1) − (row 2)
2	-1	5	(row 4) = (row 2) − (row 3)
-3	2	3	(row 5) = (row 3) − (row 4)
5	-3	2	(row 6) = (row 4) − (row 5)
-8	5	1	(row 7) = (row 5) − (row 6)
21	-13	0	(row 8) = (row 6) − 2(row 7)

From the second-to-last row we see that $13(-8)+21(5)=1$ and hence

$$\frac{1}{13\cdot 21}=\frac{5}{13}+\frac{-8}{21}.$$

(b): There are many methods to compute partial fractions of polynomials. I will use the Extended Euclidean Algorithm as in part (c). We want to find polynomials $A(x)$ and $B(x)$ such that

$$\frac{1}{(x+1)(x^2+1)}=\frac{A(x)}{x+1}+\frac{B(x)}{x^2+1}, \qquad \text{and hence} \quad 1=A(x)(x^2+1)+B(x)(x+1).$$

To do this, we consider all triples of polynomials $A(x),B(x),C(x)$ such that

$$A(x)(x^2+1)+B(x)(x+1)=C(x).$$

Beginning with the easy triples $(1,0,x^2+1)$ and $(0,1,x+1)$ we perform row operations to obtain a triple of the form $(A(x),B(x),1)$:

$A(x)$	$B(x)$	$C(x)$	operation
1	0	x^2+1	(row 1)
0	1	$x+1$	(row 2)
1	$-x+1$	2	(row 3) = (row 1) $-$ $(x-1)$(row 2)
$1/2$	$(-x+1)/2$	1	(row 4) = (row 3)/2

I performed polynomial long division to find row 3:

$$\begin{array}{r|l} & \quad\;\; x-1 \\ \hline x+1 & x^2 \qquad +1 \\ & -x^2-x \\ \hline & \qquad -x+1 \\ & \qquad\;\;\; x+1 \\ \hline & \qquad\qquad 2 \end{array}$$

Row 4 is not strictly part of the Euclidean Algorithm. It just scales the gcd to be monic. Thus we obtain

$$1=(x^2+1)(1/2)+(x+1)(-x+1)/2$$
$$\frac{1}{(x+1)(x^2+1)}=\frac{1/2}{x+1}+\frac{(-x+1)/2}{x^2+1}.$$

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.

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

(a): Suppose that $aR+bR=cR$. Since $a=a\cdot 1+b\cdot 0$ we have $a\in aR+bR$ and hence $a\in cR$. By definition this means that $a=cr$ for some $r\in R$, hence $c|a$. Switching the roles of a and b shows that $c|b$.

(b): Now consider any $d\in R$ such that $d|a$ and $d|b$. Say $a=dk$ and $b=d\ell$. Since $c\in cR$ and $cR=aR+bR$ we have $c=ax+by$ for some $x,y\in R$. Finally, we have

$$\begin{aligned} c &= ax+by \\ &= (dk)x+(d\ell)y \\ &= d(kx+\ell y), \end{aligned}$$

and hence $d|c$.

(c): Suppose that $aR+bR=c_1R$ and $aR+bR=c_2R$, so that $c_1R=c_2R$. If one of c_1 of c_2 is zero then so is the other, in which case $c_1\sim c_2$. So we assume that $c_1,c_2\neq 0$. Since $c_1\in c_1R$ we have $c_1\in c_2R$, hence $c_1=c_2u$ for some $u\in R$. Similarly, we have $c_2=c_1v$ for some $v\in R$. If R is a domain then I claim that u and v must be units. Indeed, we must have

$$\begin{aligned} c_2 &= c_1v \\ c_2 &= (c_2u)v \\ c_2(1-uv) &= 0 \\ 1-uv &= 0 && \text{since } c_2\neq 0 \\ 1 &= uv. \end{aligned}$$

Hence $c_1\sim c_2$.

Remark: This tells us that any two integers have a unique non-negative gcd and that any two polynomials over a field have a unique monic gcd (i.e., with leading coefficient 1).

5. The Euclidean Algorithm.

(a) *Missing Lemma.* Let R be a commutative ring and suppose that we have $a=bk+c$ for some elements $a,b,c,k\in R$. 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

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

Note: I changed $a=bx+c$ to $a=bk+c$ just for fun.

(a): Suppose that $a=bk+c$. To see that $aR+bR\subseteq bR+cR$ we note that an arbitrary element $ax+by\in aR+bR$ is also in $bR+cR$:

$$ax+by=(bk+c)x+by=b(kx+y)+c(x)\in bR+cR.$$

And to see that $bR+cR\subseteq aR+bR$ we note that an arbitrary element $bx+cy\in bR+cR$ is also in $aR+bR$:

$$bx+cy=bx+(a-bk)y=a(y)+b(x-ky)\in aR+bR.$$

(b): We consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ such that $32x + 47y = z$. Starting with the easy triples $(0, 1, 47)$ and $(1, 0, 32)$ we perform row operations until we obtain a triple of the form $(x, y, 1)$:

x	y	z	operation
0	1	47	(row 1)
1	0	32	(row 2)
-1	1	15	(row 3) = (row 1) $-$ 1(row 2)
3	-2	2	(row 4) = (row 2) $-$ 2(row 3)
-22	15	1	(row 5) = (row 3) $-$ 7(row 4)
47	-32	0	(row 6) = (row 4) $-$ 2(row 5)

We conclude that

$$32(-22) + 47(15) = 1.$$

Remark: There are infinitely many solutions. The complete solution is

$$32(-22 + 47k) + 47(15 - 32k) = 1 \text{ for all } k \in \mathbb{Z}.$$

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 $p|k$.]

(a): For any integers $a, b, m \in \mathbb{Z}$ with $m \geq 1$ we recall from Homework 1 that

$$\begin{aligned} a^m - b^m &= (a - b)(a^{m-1} + a^{m-2}b + \cdots + ab^{m-2} + b^{m-1}) \\ &= (a - b)(\text{some integer}), \end{aligned}$$

so that $a - b$ divides $a^m - b^m$. Now let $k = \ell m$ where $k, m \in \mathbb{Z}$ and $m \geq 1$ is **odd**. Putting putting $a = 2^\ell$ and $b = -1$ gives

$$a - b = 2^\ell + 1$$

and

$$a^m - b^m = (2^\ell)^m - (-1)^m = 2^{\ell m} - (-1)^{\text{odd}} = 2^k + 1.$$

Hence $2^\ell + 1$ divides $2^k + 1$.

(b): Suppose that k is not a power of 2. By definition, the prime factorization of k contains a prime p not equal to 2. But every prime except for 2 is odd, hence k has an odd prime factor:

$$k = \ell p \text{ for some } \ell, p \text{ where } p \text{ is odd and } p \geq 3.$$

From part (a) (with $m = p$) this implies that

$$2^\ell + 1 \text{ is a divisor of } 2^k + 1.$$

Since $2^\ell + 1 \neq 1$ and $2^\ell + 1 \neq 2^k + 1$ (because $p \neq 1$), we conclude that $2^k + 1$ has a non-trivial divisor. Hence $2^k + 1$ is not prime.

Remark: Thus we have shown that

$$2^k + 1 \text{ is prime} \quad \Longrightarrow \quad k = 2^n \text{ for some } n \geq 1.$$

This was discovered by Pierre de Fermat, who conjectured that the converse is also true:

$$k = 2^n \text{ for some } n \geq 1 \quad \Longrightarrow \quad 2^k + 1 \text{ is prime.}$$

To be precise, consider the nth *Fermat number*:

$$F_n = 2^{(2^n)} + 1.$$

Here are the first few values:

n	0	1	2	3	4
F_n	3	5	17	257	65537

Fermat observed that all of these numbers are prime and he conjectured that F_n is prime for all $n \geq 0$. Euler showed in 1732 that F_5 is **composite**:

$$F_5 = 4294967297 = 641 \cdot 6700417.$$

As of November 2021[3] we know that F_6 through F_{11} are also **composite**, and no other "Fermat prime" has ever been found. Thus Fermat's conjecture was very wrong.

Later in the course we will see the *Gauss-Wantzel Theorem*, which says the following:

> The regular n-gon can be constructed with ruler and compass if and only if $n = 2^k p_1 \cdots p_\ell$ where $p_1, \ldots, p_\ell$ are distinct Fermat primes.

[3] `https://en.wikipedia.org/wiki/Fermat_number`