Winter 2021, Math 533: Abstract Algebra Homework #2
Rose Adkisson

Problem 1. **Exercise 1**: Let R be a ring. Let a be a nilpotent element of R. (Recall that "nilpotent" means that there exists some $n \in \mathbb{N}$ such that $a^n = 0$.)

(a) Prove that $1 - a \in R$ is a unit.

(b) Let $u \in R$ be a unit satisfying $ua = au$. Prove that $u - a \in R$ is a unit.

Solution.

(a) To show that $1-a \in R$ is a unit, we must show that $1-a$ has an inverse in R. In other words, we much show that there exists some $p \in R$ such that $(1-a)p = p(1-a) = 1$. Note that $a^n = 0$ for some large enough $n \in \mathbb{N}$ since a is nilpotent. Thus $1 - a^n = 1 - 0 = 1$. We then find that if we can find p such that $1 - a^n = (1-a)p = p(1-a)$, we have found p that is inverse to $1 - a$ and therefore shown that $1 - a$ is a unit.

We may let $p = 1 + a + a^2 + ... + a^{n-1}$. Clearly $p \in R$ and

$$\begin{aligned}(1-a)p &= (1-a)(1 + a + a^2 + ... + a^{n-1}) \\ &= (1-a)\cdot 1 + (1-a)\cdot a + (1-a)\cdot a^2 + ... + (1-a)\cdot a^{n-1} \\ &= 1\cdot 1 - a\cdot 1 + 1\cdot a - a\cdot a + a\cdot a - ... - a\cdot a^{n-2} + 1\cdot a^{n-1} - a\cdot a^{n-1} \\ &= 1 - a + a - a^2 + a^2 - ... - a^{n-1} + a^{n-1} - a^n \\ &= 1 - a^n \\ &= 1.\end{aligned}$$

It is easy to see that $p(1-a)$ yields the same process and result. Thus we have found a $p \in R$ that is inverse to $1 - a$. Thus $1 - a$ is a unit of R.

(b) Since u is a unit of R, there exists some $u^{-1} \in R$ such that $uu^{-1} = u^{-1}u = 1$. Also recall that $au = ua$.

Claim: a and u^{-1} commute.
Proof:

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

Hence, $(u^{-1}a)^n = (u^{-1})^n a^n = 0$, since $a^n = 0$.
Similar to (a), we will explicitly find the inverse to $u - a$ when $a^n = 0$ for some $n \in \mathbb{N}$.

Let $p = u^{-1} + u^{-1}(u^{-1}a) + u^{-1}(u^{-1}a)^2 + ... + u^{-1}(u^{-1}a)^{n-1}$. Clearly $p \in R$ and

$$
\begin{aligned}
&(u-a)p \\
&= (u-a)(u^{-1} + u^{-1}(u^{-1}a) + u^{-1}(u^{-1}a)^2 + ... + u^{-1}(u^{-1}a)^{n-1}) \\
&= (u-a)\cdot u^{-1} + (u-a)\cdot u^{-1}(u^{-1}a) + (u-a)\cdot u^{-1}(u^{-1}a)^2 + ... + (u-a)\cdot u^{-1}(u^{-1}a)^{n-1} \\
&= uu^{-1} - au^{-1} + uu^{-1}(u^{-1}a) - au^{-1}(u^{-1}a) + ... + uu^{-1}(u^{-1}a)^{n-1} - au^{-1}(u^{-1}a)^{n-1} \\
&= 1 - u^{-1}a + u^{-1}a - (u^{-1}a)^2 + ... - (u^{-1}a)^{n-1} + (u^{-1}a)^{n-1} - (u^{-1}a)^n \\
&\qquad \big(\text{using the commutativity of } a \text{ with } u^{-1}\big) \\
&= 1 - (u^{-1}a)^n \\
&= 1 - 0 \\
&= 1.
\end{aligned}
$$

It is easy to see that $p(u-a)$ yields the same process and result. Thus we have found a $p \in R$ that is inverse to $u - a$. Thus $u - a$ is a unit of R.

□

Problem 3. **Exercise 3**: Let R be an integral domain. Let $a \in R$ and $b \in R$. Assume that a and b have an lcm $\ell \in R$. Prove that a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$.

Solution. Let R be an integral domain, $a, b \in R$, and let ℓ be an lcm of a and b. If $a = 0$, then $\ell = 0$ (since $a \mid \ell$) and therefore b is a gcd g of a and b (since $b \mid 0 = a$ and $b \mid b$) that satisfies $g\ell = ab$ (since $b\ell = 0 = ab$). Thus we are done in the case when $a = 0$. Similarly we can handle the case when $b = 0$. From now on, we assume that $a \neq 0$ and $b \neq 0$. Since R is an integral domain, this implies $ab \neq 0$. Also, since R is an integral domain, fractions of the form $\dfrac{u}{v}$ with $u \in R$ and $v \in R \setminus \{0\}$ are well-defined (i.e., unique) when $v \mid u$. The following property of such fractions will be used without saying: If $u, u' \in R$ and $v, v' \in R \setminus \{0\}$ are such that $v \mid u$ and $v' \mid u'$, then $vv' \mid uu'$ and $\dfrac{u}{v} \cdot \dfrac{u'}{v'} = \dfrac{uu'}{vv'}$.

Consider ab: this is a common multiple of a and b, since $a|ab$ and $b|ab$. Hence, $\ell|ab$ as ℓ is an lcm of a and b. Thus, $\dfrac{ab}{\ell} \in R$ is well-defined. (Indeed, $\ell|ab$ and $ab \neq 0$ yield $\ell \neq 0$.)

We will first show that $\dfrac{ab}{\ell}$ is a common divisor of a and b; then we will show that $\dfrac{ab}{\ell}$ is a gcd g of a and b that satisfies $ab = g\ell$.

- Showing that $\dfrac{ab}{\ell}$ is a common divisor of a and b: We have $\dfrac{\ell}{b} \in R$ (since $b|\ell$). Now,

$$a = \frac{ab\ell}{\ell b} = \frac{ab}{\ell} \cdot \frac{\ell}{b}.$$

  Since $\dfrac{\ell}{b} \in R$, this entails

$$\frac{ab}{\ell} \Big| a.$$

  Similarly, we find

$$\frac{ab}{\ell} \Big| b.$$

  Thus we have that $\dfrac{ab}{\ell}$ is a common divisor of a and b.

- Showing that $\dfrac{ab}{\ell}$ is a gcd of a and b: We must show that, for any common divisor d of a and b, we have $d|\dfrac{ab}{\ell}$.

  Suppose $d \in R$ is a common divisor of a and b. Then $d|a$ and $d|b$, so $d|ab$. Hence, $\dfrac{ab}{d} \in R$. Since $d|b$, we find $\dfrac{b}{d} \in R$, and thus

$$a \Big| \left(a \cdot \frac{b}{d} \right) = \frac{ab}{d}.$$

  Similarly, $b \Big| \dfrac{ab}{d}$. Therefore, $\dfrac{ab}{d}$ is a common multiple of a and b. Thus, as ℓ is an lcm of a and b, we have

$$\ell \Big| \frac{ab}{d}.$$

Thus there exists some $k \in R$ with $\ell k = \dfrac{ab}{d}$, implying $d\ell k = ab$ and therefore $dk = \dfrac{ab}{\ell}$. Thus

$$d \Big| \frac{ab}{\ell}.$$

We have now shown that any common divisor d of a and b is a divisor of $\dfrac{ab}{\ell}$. This gives that $\dfrac{ab}{\ell}$ is a gcd of a and b.

Thus, $\dfrac{ab}{\ell}$ is a gcd of a and b. Of course, if we denote it by g, then it satisfies $ab = g\ell$ (by its definition). We have now shown all of the desired claims.

□

Problem 5. **Exercise 5**: Let p be a prime number.

(a) Prove that the only units of the ring $\mathbb{Z}/p$ that are their own inverses (i.e., the only $m \in (\mathbb{Z}/p)^\times$ that satisfy $m^{-1} = m$) are $\overline{1}$ and $\overline{-1}$.

(b) Assume that p is odd. Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Prove that $u!^2 \equiv -(-1)^u \mod p$.

Solution.

(a) Consider any unit $r \in \mathbb{Z}/p$ where $r = r^{-1}$. We will show that $r = 1$ or $r = -1$ (where 1 means $1_{\mathbb{Z}/p} = \overline{1}$).
We have $rr^{-1} = 1$. Since $r = r^{-1}$, this rewrites as $rr = 1$. In other words, $r^2 = 1$, so that $r^2 - 1 = 0$. This rewrites as $(r-1)(r+1) = 0$. But $\mathbb{Z}/p$ is a field and thus an integral domain; hence, all nonzero $a, b \in \mathbb{Z}/p$ satisfy $ab \neq 0$. Thus, since $(r-1)(r+1) = 0$, we hve either $r - 1 = 0$ or $r + 1 = 0$. Thus, $r = 1$ or $r = -1$. This shows that the only units of the ring $\mathbb{Z}/p$ that are their own inverses are $1 = \overline{1}$ and $-1 = \overline{-1}$.

(b) Since p is odd, we have

$$(p-1)! = (p-1) \cdot (p-2) \cdot ... \cdot \frac{p+1}{2} \cdot \frac{p-1}{2} \cdot ... \cdot 2 \cdot 1.$$

We will now look to rewrite the first half of these factors modulo p:

$$\begin{aligned} p - 1 &\equiv -1 \mod p; \\ p - 2 &\equiv -2 \mod p; \\ &...; \\ \frac{p+1}{2} = p - \frac{p-1}{2} &\equiv -\frac{p-1}{2} \mod p. \end{aligned}$$

Thus we may rewrite $(p-1)!$ as follows:

$$(p-1)! \equiv (-1) \cdot (-2) \cdot ... \cdot \left(-\frac{p-1}{2}\right) \cdot \frac{p-1}{2} \cdot ... \cdot 2 \cdot 1 \mod p.$$

Notice that there are $\dfrac{p-1}{2}$ negative factors and $\dfrac{p-1}{2}$ positive factors on the right hand side, and the each of the former agrees with exactly one of the latter in its absolute value. Thus, by combining factors with equal absolute value, we can rewrite the above as follows:

$$(p-1)! \equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdot ... \cdot \frac{p-1}{2}\right)^2 \mod p.$$

This rewrites as

$$(p-1)! \equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)!^2 \mod p.$$

By Wilson's Theorem, we have that $(p-1)! \equiv -1 \mod p$, so that

$$-1 \equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)!^2 \mod p;$$

in other words,

$$\left(\frac{p-1}{2}\right)!^2 \equiv -1(-1)^{(p-1)/2} \mod p.$$

Recalling that $u = \frac{p-1}{2}$, we can rewrite this as

$$u!^2 \equiv -1(-1)^u \mod p,$$

which is our desired result.

□

Problem 8. **Exercise 8**: Let R be a ring. Let I and J be two ideals of R such that $I \subseteq J$. Let J/I denote the set of all cosets $j + I \in R/I$ where $j \in J$. Prove the following:

(a) This set J/I is an ideal of R/I.

(b) We have $(R/I)\,/\,(J/I) \cong R/J$ (as rings). More concretely, there is a ring isomorphism $R/J \to (R/I)\,/\,(J/I)$ that sends each residue class $\overline{r} = r+J$ to $\overline{r+I} = (r+I)+(J/I)$.

Solution.

(a) To be an ideal of R/I, the set J/I must be a subset of R/I such that

1. $a + b \in J/I$ for all $a, b \in J/I$;
2. $ab \in J/I$ and $ba \in J/I$ for all $b \in J/I$ and all $a \in R/I$;
3. $0_{R/I} \in J/I$.

First note that it is clear that $J/I \subset R/I$ by definition of J/I.

Next we will address (1), that is, the claim that J/I is closed under addition. Consider any $j_1 + I, j_2 + I \in J/I$ (with $j_1, j_2 \in J$). Then $j_1 + I + j_2 + I = (j_1 + j_2) + I$. Since J is an ideal, it is closed under addition, thus $j_1 + j_2 \in J$. Thus $(j_1 + j_2) + I \in J/I$ and J/I is closed under addition. Thus (1) is proved.

Next we must prove (2), i.e., show that the product of an element of J/I and an element of R/I remains in J/I. Consider any $j + I \in J/I$ (with $j \in J$) and any $r + I \in R/I$. Then

$$(j + I)(r + I) = jr + I.$$

Note that J is an ideal of R and is therefore closed under multiplication with an element of R, so $jr \in J$. Thus $jr + I \in J/I$. Also note

$$(r + I)(j + I) = rj + I.$$

Note that J is an ideal of R and is therefore closed under multiplication with an element of R, so $rj \in J$. Thus $rj + I \in J/I$. Thus (2) is proved.

Since J is an ideal of R, we have $0_R \in J$. Thus $0_R + I \in J/I$. Also note $0_{R/I} = 0_R + I$. Thus $0_{R/I} \in J/I$.

We have now shown the properties necessary for J/I to be an ideal of R/I.

(b) Consider the map $f : R/I \to R/J$, $r + I \mapsto r + J$. First we need to show that f is well defined:

For $r_1 + I, r_2 + I \in R/I$, if $r_1 + I = r_2 + I$, we must show that $r_1 + J = r_2 + J$. We will use the fact that $I \subset J$:

$$\begin{aligned} r_1 + I = r_2 + I &\implies r_1 - r_2 \in I \\ &\implies r_1 - r_2 \in J \\ &\implies r_1 + J = r_2 + J. \end{aligned}$$

It is obvious that the map f respects addition, multiplication, the zero, and the unity; thus, f is a ring morphism. Now, by the *First Isomorphism Theorem for Rings*, we have

$$(R/I)/\ker f \cong f(R/I). \tag{1}$$

Next we will show that f is surjective, giving $f(R/I) = R/J$.

Consider any $r+J \in R/J$. We can find a preimage for it, namely $r+I \in R/I$. Thus every element of R/J has a preimage and f is surjective.

Thus (1) becomes

$$(R/I)/\ker f \cong R/J. \tag{2}$$

As our last step to achieving the desired result, we will show that $\ker f = J/I$.

Let $r + I \in \ker f$. Then $f(r + I) = 0 + J$. But $f(r + I) = r + J$. Thus $0 + J = r + J$ and therefore $r \in J$. Thus $r + I \in J/I$. Thus we have shown that $\ker f \subset J/I$.

Let $r+I \in J/I$ with $r \in J$. Then $r+J = 0+J$. Thus $f(r+I) = r+J = 0+J$ and therefore $r + I \in \ker f$. Thus $J/I \subset \ker f$.

Thus $J/I = \ker f$.

Hence, (2) becomes

$$(R/I)/(J/I) \cong R/J.$$

Moreover, the isomorphism $(R/I)/(J/I) \to R/J$ constructed by the *First Isomorphism Theorem for Rings* sends each $(r + I) + (J/I) = (r + I) + \ker f \in (R/I)/(J/I)$ to $f(r + I) = r + J \in R/J$. Hence, its inverse sends each $r + J$ to $(r + I) + (J/I)$, as claimed in the exercise.

□

Problem 9. **Exercise 9**: Let R be a ring. Let S be a subring of R. Let I be an ideal of R. Define $S + I$ to be the subset $\{s + i \mid s \in S \text{ and } i \in I\}$ of R.

Prove the following:

(a) This subset $S + I$ is a subring of R.

(b) The set I is an ideal of the ring $S + I$.

(c) The set $S \cap I$ is an ideal of the ring S.

(d) We have $(S + I)/I \cong S/(S \cap I)$ (as rings). More concretely, there is a ring isomorphism $S/(S \cap I) \to (S + I)/I$ that sends each residue class $\overline{s} = s + (S \cap I)$ to $\overline{s} = s + I$.

Solution.

(a) Since S is a subring of R and I is an ideal of R, first note that it is obvious that $S + I \subset R$. Next it is clear that $S + I := \{s + i | s \in S, i \in I\}$ contains the unity of R, the zero of R, and respects addition. Thus we will simply show that $S + I$ respects negation and multiplication.

Consider any $a, b \in S + I$. Thus, $a = s_1 + i_1$ and $b = s_2 + i_2$ for some $s_1, s_2 \in S$ and $i_1, i_2 \in I$. We then have

$$a - b = (s_1 + i_1) - (s_2 + i_2) = (s_1 - s_2) + (i_1 - i_2).$$

Note that $s_1 - s_2 \in S$ as S is a ring, and $i_1 - i_2 \in I$ as I is an ideal. Thus we have $(s_1 - s_2) + (i_1 - i_2) \in S + I$. That is, $a - b \in S + I$. This shows that $S + I$ is closed under subtraction, hence closed under negation (since $0 \in S + I$).

Consider any $a, b \in S + I$. Thus, $a = s_1 + i_1$ and $b = s_2 + i_2$ for some $s_1, s_2 \in S$ and $i_1, i_2 \in I$. Then,

$$ab = (s_1 + i_1)(s_2 + i_2) = s_1 s_2 + s_1 i_2 + i_1 s_2 + i_1 i_2.$$

Note $s_1 s_2 \in S$ as S is a ring and closed under multiplication. Also note $s_1 i_2 + i_1 s_2 + i_1 i_2 \in I$ since I is an ideal and is therefore closed under multiplication with all elements of R and closed under addition as well. Thus $s_1 s_2 + s_1 i_2 + i_1 s_2 + i_1 i_2 \in S + I$. In other words, $ab \in S + I$. Thus $S + I$ is closed under multiplication.

Since $S + I$ contains the unity of R, contains the zero of R, is closed under addition, is closed under negation, and is closed under multiplication, we conclude that $S + I$ is a subring of R.

(b) To be an ideal of $S + I$, the set I must be a subset of $S + I$ such that

1. $a + b \in I$ for all $a, b \in I$;
2. $ab \in I$ and $ba \in I$ for all $b \in I$ and all $a \in S + I$;
3. $0_{S+I} \in I$.

First note that it is obvious that $I \subset S + I$, since $0 \in S$.

Next, since I is an ideal of R and $S + I$ is a subring of R, we find that I inherits the properties of closure under addition and containing $0_R = 0_{S+I}$. Thus all we must

check is for any $b \in I$ and any $a \in S + I$ that $ab \in I$ and $ba \in I$.

Consider any $b \in I$ and any $a \in S + I$. Write $a \in S + I$ as $a = s + i$ with $s \in S$ and $i \in I$. Then

$$ab = (s + i)b = sb + ib \in I$$

(indeed, since I is closed under multiplication with elements of R, we have $sb \in I$ and $ib \in I$, and therefore we get $sb + ib \in I$ because I is closed under addition). Similarly $ba \in I$. We have now shown the properties necessary for I to be an ideal of $S + I$.

(c) To be an ideal of S, the set $S \cap I$ must be a subset of S such that

1. $a + b \in S \cap I$ for all $a, b \in S \cap I$;
2. $ab \in S \cap I$ and $ba \in S \cap I$ for all $b \in S \cap I$ and all $a \in S$;
3. $0_S \in S \cap I$.

First note that it is clear $S \cap I \subset S$.

It should also be clear, since S is a subring of R, that $0_S = 0_R$ and $0_R \in S$. Since I is an ideal of R, we have $0_R \in I$. Thus $0_R \in S \cap I$. In other words, $0_S \in S \cap I$.

Next we will address (1), that is, the claim that $S \cap I$ is closed under addition. Let $a, b \in S \cap I$. Then $a, b \in S$ and $a, b \in I$. Since S is closed under addition as a ring, we find $a + b \in S$. Since I is an ideal of R, I is also closed under addition, so that $a + b \in I$. Thus $a + b \in S \cap I$.

Next we must prove (2), i.e., show that the product of an element of $S \cap I$ and an element of S remains in $S \cap I$. Let $b \in S \cap I$ and let $a \in S$. Then $b \in S$, $b \in I$, and $a \in S \subset R$. Since I is an ideal of R, it is closed under multiplication with elements of R; thus, $ab, ba \in I$. Since S a ring, it is closed under multiplication, so we conclude from $a \in S$ and $b \in S$ that $ab, ba \in S$. Thus we have $ab, ba \in S \cap I$.

We have now shown the properties necessary for $S \cap I$ to be an ideal of S.

(d) Consider the map $f : S \to (S + I)/I$, $s \mapsto s + I$. We will show that f is a ring morphism. First note that S is a ring, as is $(S + I)/I$ by parts **(a)** and **(b)**. Next we note that f clearly respects addition, multiplication, the zero, and the unity; therefore, f is a ring morphism. Hence, by the *First Isomorphism Theorem for Rings*, we have

$$S/\ker f \cong f(S). \tag{3}$$

Next we will show that f is surjective, giving $f(S) = (S + I)/I$.

> To show that f is surjective, we must show that every element of $(S + I)/I$ has a preimage in S. Let $a+I \in (S+I)/I$. Thus, $a \in S+I$, so that $a = s+i$ for some $s \in S$ and $i \in I$. Hence, $a+I = s+I$ (since $a = s+i \in s+I$). Now, the definition of f shows that $f(s) = s + I = a + I$. This shows that $a + I$ has a preimage in S. Thus, we have shown that each element of $(S + I)/I$ has a preimage, so that f is surjective.

Since f is surjective, have $f(S) = (S + I)/I$, so that we can rewrite (3) as

$$S/\ker f \cong (S + I)/I. \tag{4}$$

As our last step to achieving the desired result, we will show that $\ker f = S \cap I$.

Let $s \in \ker f$. Then $f(s) = 0 + I$. But $f(s) = s + I$, so $s + I = 0 + I$. Thus $s \in I$. Also note that the kernel is a subset of the domain S, thus $s \in S$. Thus we have $s \in S \cap I$. This proves that $\ker f \subset S \cap I$.

Let $s \in S \cap I$. Then $s \in S$ and $s \in I$. Then $f(s) = s + I$. Since $s \in I$, we have $s + I = 0 + I$. Thus $f(s) = 0 + I$. Thus $s \in \ker f$. This proves $S \cap I \subset \ker f$.

Thus $S \cap I = \ker f$.

Hence, (4) rewrites as

$$S/(S \cap I) \cong (S + I)/I.$$

Moreover, the isomorphism $S/(S \cap I) \to (S + I)/I$ constructed by the *First Isomorphism Theorem for Rings* sends each $s+(S \cap I) \in S/(S \cap I)$ to $f(s) = s+I \in (S+I)/I$, as claimed in the exercise.

□