Math 310: Fall 2025: Solutions to Homework

Steven Miller

November 18, 2025

Abstract

Below are detailed solutions to the homework problems from Math 310 Introduction to Modern Algebra (Siena University, Fall 2025, Professor Steven J. Miller, sjm1@williams.edu). The course homepage is

https://web.williams.edu/Mathematics/sjmiller/public_html/310Fa25/

and the textbook is *Abstract Algebra: An Integrated Approach* by Joseph Silverman (ISBN13: 978-1470468606).

Note to students: it's nice to include the statement of the problems, but I leave that up to you. **I will occasionally add some comments or mention alternate solutions. If you find an error in these notes, let me know for extra credit.** Solutions are due to many, including Theo Mollano, Steven J. Miller, Joeseph Silverman, Matthew Wu, and Sam Chistolini.

Contents

1 Homework 1 **2**

2 Homework 2 **2**

3 Homework 3 **7**

4 Homework 4 **13**

5 Homework 5 **22**

6 Homework 7 **33**

1 Homework 1

Due Date: September 3
Problems:

Homework: To be emailed to me by 10pm on Wednesday, Sept 3rd: Email me a short note on what you want to get out of this course, and what lesson you learned from the graduation speech (https://whatrocks.github.io/commencement-db/2006-michael-uslan-indiana-university/) (ted talk version here: https://www.youtube.com/watch?v=7LUg-7zDWHo&t=534s). Full credit, 20/20, so long as you answer both questions on time. General life advice: strongly encourage you not to wait till the last minute to do things.

Homework: Read Chapter 1 for Thursday's class. Email me with any questions you have on the material (much of it should be review). I will emphasize proofs by induction and the binomial theorem if there are not a lot of questions. You are encouraged to read the first few sections of Chapter 2, as we will discuss those starting on Thursday; if there is time on Tuesday after covering Chapter 1 I will cover some of the cryptography material that we will see later in the semester.

2 Homework 2

Due Date: Thursday, September 11
Problems:

1. Prove by induction that the sum of the first n odd numbers is n^2.
2. Prove $\binom{n}{k} = \binom{n}{n-k}$.
3. What should $\binom{3}{5}$ equal? Based on your answer to this, what should the factorial of a negative integer be?
4. Problem 1.12: Let $\mathcal{S}$ be the set $\mathcal{S} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and define an equivalence relation on $\mathcal{S}$, $a \sim b$ if and only if $a - b$ is even. (a) Prove that this is an equivalence relation on $\mathcal{S}$. (b) Write $\mathcal{S}$ as a disjoint union of the equivalence classes for the equivalence relation.
5. Problem 1.16: Give an example of a function from the natural numbers to the natural numbers that is (a) injective but not surjective and (b) surjective but not injective.

Solutions next page

Homework 2: Solutions

Problem (1)**.** *Prove by induction that the sum of the first n odd numbers is n^2.*

Solution. We induct on N and show that

$$\sum_{n=1}^{N}(2n-1) \;=\; N^2$$

for any $N \in \mathbb{N}$.

We first verify the base case $N = 1$. We have $1 = 1^2$, proving the claim.

For our inductive hypothesis, we assume that for some $N \geq 1$, $\sum_{n=1}^{N}(2n-1) = N^2$ We must now show it holds for $N+1$. We have

$$\begin{aligned}\sum_{n=1}^{N+1}(2n-1) \;&=\; \Big(\sum_{n=1}^{N}2n-1\Big)+(2(N+1)-1)\\ &=\; N^2+2N+1\\ &=\; (N+1)^2,\end{aligned}$$

which gives the desired result. □

Problem (2)**.** *Prove* $\binom{n}{k} = \binom{n}{n-k}$.

Solution. Our first proof is just brute force algebra from the definition of the binominal coefficients:

$$\begin{aligned}\binom{n}{k} \;&=\; \frac{n!}{k!(n-k)!}\\ &=\; \frac{n!}{(n-k)!(n-(n-k))!}\\ &=\; \binom{n}{n-k},\end{aligned}$$

as desired.

We can give a "better" proof by telling a story (this proof is better as it gives a reason why the result is true, and not just the consequence of doing some algebra). We note that $\binom{n}{k}$ gives the number of ways to choose exactly k objects from a set containing n elements when order does not matter. We could alternatively view this process as we are choosing to exclude exactly $n-k$ elements, and the number of ways to do that is $\binom{n}{n-k}$. Thus, the number of ways of excluding exactly $n-k$ elements is the same as that of choosing exactly

k elements. □

Problem (3)**.** *What should $\binom{3}{5}$ equal? Based on your answer to this, what should the factorial of a negative integer be?*

Solution. We claim $\binom{3}{5} = 0$. By definition, we know that $\binom{n}{k}$ gives the number of ways of choosing exactly k elements from a total of n elements when order does not matter. As there is no way to take 5 elements from a set containing 3 elements, this must be zero.

From this, we see a natural way to define the "factorial" of negative integers (although this doesn't have any particular combinatorial significance). If we wish the algebraic formula for $\binom{n}{k}$ to still hold in this case, we need

$$\frac{3!}{5!(-2)!} \;=\; \text{or} \;\; \frac{6}{120(-2)!} \;=\; 0$$

For this to hold, we must divide by infinity (no finite number will do!), and thus the above implies the factorial of a negative integer is ∞ (up to sign of course!).

Remark 2.1 (Advanced)**.** *In fact, there is a beautiful generalization of the factorial formula, namely the Gamma function. It is defined as*

$$\Gamma(s) \;:=\; \int_0^\infty x^{s-1}e^{-x}dx$$

for $\Re(s) > 0$. Simple integration by parts shows that $\Gamma(s+1) = s\Gamma(s)$. This gives back our original factorial formula if $s \in \mathbb{N}$. The gamma function $\Gamma(s)$ has simple poles only at negative integers. We can even push this further and show this holds for all s except negative integers by the power of analytic continuation. As a nice fact, we have

$$\Gamma(1/2) \;=\; \sqrt{\pi}.$$

Note this does not mean the number of ways of ordering negative one-half of a person is the square-root of π; we only have that interpretation for the factorial of non-negative integers.

□

Problem (4)**.** *Let $\mathcal{S}$ be the set $\mathcal{S} = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and define an equivalence relation on $\mathcal{S}$, $a \sim b$ if and only if $a - b$ is even. (a) Prove that this is an equivalence relation on $\mathcal{S}$. (b) Write $\mathcal{S}$ as a disjoint union of the equivalence classes for the equivalence relation.*

Solution. We first show that $\sim$ is indeed an equivalence relation. Let $a, b \in \mathcal{S}$, we see the following properties hold:

(a) $a \sim b$ is indeed reflexive. We observe that $a \sim a$ as $a - a = 0$, which is an even number.

(b) $a \sim b$ is indeed symmetric. If $a \sim b$ that means $a - b = 2n$ for some integer n, but as $a - b = -(b - a) = -2n$, which implies that $b - a$ is also even, and thus $a \sim b$ implies $b \sim a$.

(c) $a \sim b$ is transitive. Suppose we have $a \sim b$ and $b \sim c$. Then $a - b$ and $b - c$ are both even. Observe that

$$a - c \;=\; a + (-b + b) - c \;=\; (a - b) + (b - c),$$

which is indeed even as it is the sum of two even numbers. Thus, we have $a \sim c$.

We can see the following equivalence classes hold:

$$[1] \;=\; \{1, 3, 5, 7\} \qquad [2] \;=\; \{2, 4, 6, 8\}.$$

We indeed see they are disjoint, *i.e.*, $[1] \cap [2] = \emptyset$. Their union is given by

$$[1] \cup [2] \;=\; \mathcal{S}$$

as desired.

Remark 2.2. *It is worth noting that the proof of transitivity used a very common "trick" – do nothing! Professor Peter Jones of Yale used to say there are two ways to do nothing: you can add zero (here represented by $-b + b$) and you can multiply by 1. (He later mused that since the logarithm of 1 is 0 there really is just one way to do nothing....) Think back to other proofs that you've seen using this technique; good examples are differentiation rules (add zero for the derivative of a sum, multiply by 1 for the chain rule, ...).*

□

Problem (5)**.** *Give an example of a function from the natural numbers to the natural numbers that is (a) injective but not surjective and (b) surjective but not injective.*

Solution. Define the function $f : \mathbb{N} \to \mathbb{N}$. We first construct a function f that is injective but not surjective. We claim $f(n) = 2n$ gives the desired property. We first show it is injective. Suppose for some $n_1, n_2 \in \mathbb{N}$ we have

$$f(n_1) \;=\; f(n_2), \quad \text{which implies} \quad 2n_1 \;=\; 2n_2.$$

Multiplying by $1/2$ on both sides, this then gives $n_1 = n_2$, proving f is injective.

Our function f is clearly not surjective, since there does not exist $n \in \mathbb{N}$ such that $f(n) = 3$ (or any odd number).

We next construct a function f that is surjective but not injective. We claim the function $f(n) = \left\lfloor \dfrac{n}{2} \right\rfloor$ has the desired property. We see it is not injective, since $f(4) = f(5) = 2$. We also see that it is surjective. To do so, we must show given any m there is an n such that $f(n) = m$. Choose n to be $2m$ gives the desired input going to the desired output. □

3 Homework 3

Due Date: Tuesday, September 30, 2025
Problems:

1. Find two elements in S_3 that do not commute.

2. Let G be a finite group whose only subgroups are $\{e\}$ and G. Prove that either $G = \{e\}$ or else that G is a cyclic group whose order is prime. Hint: Use Cauchy's Theorem. (Problem 2.38)

3. Let G be a finite group. Let K and H be subgroups of G, so that K is a subset of H which is a subset of G. Prove the index multiplication rule: $(G : K) = (G : H)(H : K)$ using Lagrange's Theorem.

4. Let G be a group, let g and h be elements of G and suppose that g has order n and that h has order m. (a) If G is an abelian group and if $\gcd(m, n) = 1$, prove that the order of gh is mn. (b) Give an example showing that (a) may not be true if we allow $\gcd(m, n) > 1$. (c) Give an example of a non-abelian group showing that (a) may not be true even if we retain the requirement that $\gcd(m, n) = 1$. (d) Assume that G is an abelian group, and let $l = mn/\gcd(m, n)$. Prove that G has an element of order l.

5. Let G be a group. The center of G, denoted $Z(G)$, is the set of elements of G that commute with every other element. $Z(G) = \{g \in G : gh = hg \text{ for every } h \text{ in } G\}$. (a) Prove that $Z(G)$ is a subgroup of G. (b) When does $Z(G)$ equal G? (Problem 2.35ab)

NOTE: I AM NOT ASSIGNING MANY PROBLEMS. YOU ARE STRONGLY ENCOURAGED TO LOOK AT OTHER PROBLEMS WITH YOUR CLASSMATES, WITH THE TA, WITH ME.

Solutions next page

Homework 3: Solutions

Problem (1)**.** *Find two elements in S_3 that do not commute.*

Solution. We would like to find two elements $x, y \in S_3$, so that $xy \neq yx$. Let $x = (1,2,3)$ (this is a cyclic permutation that sends 1 to 2, 2 to 3 and 3 to 1) and $y = (1,3)(2)$ (this is a transposition that sends 1 to 3 and 3 to 1, and leaves 2 alone).

Notice that $(1,3)(2) \circ (1,2,3) = (1,2)(3)$. To see this, we need to just look at what $(1,3)(2) \circ (1,2,3)$ does to each of the three elements. We first act with $(1,2,3)$ and then with $(1,3)(2)$. We have 1 goes to 2 and then is left alone at 2 so the net effect is 1 goes to 2, 2 goes to 3 and then 3 goes to 1 and thus 2 goes to 1, and finally 3 goes to 1 and 1 goes to 3 so the net effect is 3 goes to 3, thus $(1,3)(2) \circ (1,2,3)$ is the same as $(1,2)(3)$.

Arguing similarly we find $(1,2,3) \circ (1,3)(2) = (2,3)(1)$; thus these are not the same.

Note: sometimes we depict these transformations by $\binom{123}{231}$ and $\binom{123}{321}$.

Remark 3.1. *We will in fact prove that $S_3 \cong D_3$. That is, S_3 behaves exactly like the symmetries of a triangle. In that isomorphism, $\phi(\rho) = (1,2,3)$ and $\phi(\psi_2) = (1,3)(2)$. Justify to yourself that in D_3, $\rho\psi_2 \neq \psi_2\rho$.*

□

Problem (2)**.** *Let G be a finite group whose only subgroups are $\{e\}$ and G. Prove that either $G = \{e\}$ or else that G is a cyclic group whose order is prime. Hint: Use Cauchy's Theorem.*

Solution. Suppose G is the trivial group, then the only subgroup in G is $\{e\}$, so we are done. Otherwise, if $|G| > 1$, we first consider the case when $|G| = p$, for some prime p. Then by *Cauchy's Theorem*, $|G|$ is cyclic. It follows that the only subgroups in G are $\{e\}$ and G .

We the eliminate the case that $|G|$ is not a prime. This means $|G|$ has more than one prime in its factorisation. Then we can apply Cauchy's Theorem to each of these primes, and find that $|G|$ has more than one subgroup, a contradiction.

Remark 3.2. *We can also prove without appealing to Cauchy's theorem. Assume $G \neq \{e\}$; choose any $g \in G$ such that $g \neq e$. Then $\langle g \rangle$ is a subgroup of G, but since the only subgroups of G are itself and $\{e\}$, this has to be all of G, which means G is cyclic as $\langle g \rangle$ is cyclic. Next, we get that $|G|$ must be prime, as if not, then $|G| = p_1^{m_1} \cdot p_2^{m_2} \cdots p_n^{m_n}$ for primes $p_1, \cdot, p_n$, and positive integers $m_1, \ldots, m_n$, then it follows that $\langle g^{p_1} \rangle$ is a subgroup that is strictly contained in G, a contradiction, therefore the order of G must be prime.*

□

Problem (3)**.** *Let G be a finite group. Let K and H be subgroups of G, so that K is a subset of H which is a subset of G. Prove the index multiplication rule: $(G : K) = (G : H)(H : K)$ using Lagrange's Theorem.*

Solution. By *Lagrange's Theorem*, we have $|G| = (G : H)|H|$ (note $|G| = \#G$) and $|G| = (H : K)|K|$. Thus

$$|G| = (G : H)|H| = (G : H)(H : K)|K| \quad \text{and} \quad |G| = (G : K)|K|.$$

As K contains e it is not empty so we may divide both sides by $|K|$ (which is finite) and obtain $(G : K) = (G : H)(G : K)$. □

Problem (4)**.** *Let G be a group, let g and h be elements of G and suppose that g has order n and that h has order m. (a) If G is an abelian group and if $\gcd(m, n) = 1$, prove that the order of gh is mn. (b) Give an example showing that (a) may not be true if we allow $\gcd(m, n) > 1$. (c) Give an example of a non-abelian group showing that (a) may not be true even if we retain the requirement that $\gcd(m, n) = 1$. (d) Assume that G is an abelian group, and let $l = mn/\gcd(m, n)$. Prove that G has an element of order l.*

Solution. For part (a), let k denotes the order of gh. We first show that $k \mid mn$. We have by simple algebra (since the group is abelian)

$$(gh)^{mn} = g^{mn}h^{mn} = (g^n)^m(h^m)^n = e.$$

Thus, by **Proposition 2.13** from the textbook, we see that k divides mn, so $k \leq mn$. Next, we show $k \geq mn$. By assumption, we have

$$e = (gh)^k \implies e^n = \Big((gh)^k\Big)^n \implies e = h^{kn}.$$

We know h has order of m, so this means $m \mid kn$. By a similar argument for g, we have $n \mid km$. Since we have $\gcd(m, n) = 1$, we must have $n \mid k$ and $m \mid k$. Since $\gcd(m, n) = 1$, we can then deduce $mn \mid k$. This implies $mn \leq k$, and we previously have shown $mn \geq k$. This completes the proof that the order of gh is k.

Remark 3.3. *Are there other ways to prove this? What if we write $n = q_1k + r_1$ and $m = q_2k + r_2$ with $0 \leq r_1, r_2 < k$; can we get the result from this?*

For part (b), let's work in the unit group $((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$. Consider $\langle 2\rangle$, and $\langle 4\rangle$. The powers of 2 in the group go $\bmod 7$ as $2, 4, 1$, so $2^3 \equiv 1 \mod 7$. So, we can regard 2 as having order 3 in the group. The powers of 4 in the group go as $4, 2, 1$, so $4^3 \equiv 1 \mod 7$. So, we can regard $\langle 4\rangle$ as having order 3 in the group. However, powers of 8 are always equal to $1 \bmod 7$. So $8 = 4 \cdot 2$ has order 1. That violates our theorem.

For part (c), we can think about the dihedral group D_3. In the textbook, the dihedral group was introduced as a group consisting of three rotation ρ_i elements, and three "flipping" elements, ψ_i. Another way of thinking about D_3 is that it is the group generated by all combinations of a number of rotations a, and a single vertical

"flip", b. If we want to construct any flip around any of the three symmetries of the triangle, we rotate the triangle to the position where the flip makes sense, and then rotate back. The presentation for this group is

$$D_3 \;=\; \langle a, b : a^3 = e, b^2 = e, ab = ba^{-1} \rangle. \tag{3.1}$$

Finally, for all dihedral groups, the property $b^{-1}ab = a^{-1}$ holds. This property encodes the underlying relationship between reflections, and rotations. Now, we know that D_3 is not abelian, a has order 3, b has order 2, and $(ab)^2 = abab = ba^{-1}ab = b^2 = e$, so ab has order 2. That violates our theorem.

For an explicit example for (c), let's revisit the first problem. Consider the cyclic permutation $\binom{123}{231}$ and the transposition $\binom{123}{321}$. The first element has order 3, the second has order 2, and thus their orders are relatively prime. However, the product of the two is the permutation

$$\binom{123}{231}\binom{123}{321} \;=\; \binom{123}{132},$$

which is just a transposition of 2 and 3, and has order 2. Thus the order of the product is 2, not 6.

For part (d), we offer two different proofs:

Proof 1. G contains an element of order m, and an element of order n. Therefore, by *Lagrange's Theorem*, m and n divide the order of G, so $\operatorname{lcm}(m,n) = mn/\gcd(m,n)$ must also divide the order of G. We now apply *Converse of Lagrange's Theorem*, which holds for finite abelian groups, to see that we indeed have an element of order $\operatorname{lcm}(m,n)$.

Proof 2. We prove by employing unique factorization. Let p_i be the sequence of primes appearing in the prime factorization of m and n, where we define the index $i \in \{1, \ldots, K\}$. We have the following

$$m \;=\; \prod_{i=1}^{K} p_i^{m_i} \qquad\qquad n \;=\; \prod_{i=1}^{K} p_i^{n_i},$$

where $m_i, n_i \geq 0$. We thus can re-write their greatest common divisor and least common multiple as

$$\gcd(m,n) \;=\; \prod_{i=1}^{K} p_i^{\min(m_i,n_i)} \qquad\qquad \operatorname{lcm}(m,n) \;=\; \prod_{i=1}^{K} p_i^{\max(m_i,n_i)}. \tag{3.2}$$

The hope is to express $\operatorname{lcm}(m,n)$ in terms of divisors of m and n. This can be achieved by

$$\begin{aligned} M_1 \;&:=\; \prod_{i:m_i \geq n_i} p_i^{m_i} \qquad & M_2 \;&:=\; \prod_{i:m_i < n_i} p_i^{m_i} \\ N_1 \;&:=\; \prod_{i:n_i > m_i} p_i^{n_i} \qquad & N_2 \;&:=\; \prod_{i:n_i \leq m_i} p_i^{n_i} \quad , \end{aligned}$$

where we indeed see

$$m \;=\; M_1 M_2 \qquad n \;= N_1 N_2.$$

This allows us to rewrite least common multiple in an enlightening way:

$$\operatorname{lcm}(m,n) \;=\; M_1 N_1,$$

where $\gcd(m_1, n_1) \;:=\; 1$. We can then choose

$$g_1 := g^{n/N_1} \qquad h_1 := h^{m/M_1},$$

and we observe the orders of g_1, h_1 are well-defined, since N_1 and M_1 divide n and m by construction. Thus, if we take the product of them, we get

$$(g_1 h_1)^{\operatorname{lcm}(m,n)} \;=\; (g_1 h_1)^{M_1 N_1} \;=\; (g^{n/N_1} h^{m/M_1})^{m_1 n_1} \;=\; e$$

as desired.

Remark 3.4 (Problem Solving Insight)**.** *A big mistake one could make in doing math is to misapply the theorems. In this context, it is possible that you may think that showing $(gh)^{mn} = e$ is sufficient for proving the group has an element of order mn. Careful reading of* ***Proposition 2.13*** *shows that this is not true, since the theorem only says that the order of gh (which is unknown) divides mn. What we need to do in (a) is to prove $k = mn$, where k denotes the order of gh; this means we need to show $k \geq mn$ and $k \leq mn$. The key takeaway is we should always make sure we are careful with the consequences and limitations of a result.*

Remark 3.5 (Meta-analysis of the problem)**.** *When looking at the conditions in the question, we should always ask how necessary the condition is. Take the restriction $\gcd(m,n) = 1$ from question (a) as an example. We should rather ask whether this restriction is necessary at all; sometimes, we just use some strong properties to make our proof easier. It turns out that it is quite necessary. Suppose instead $\gcd(m,n) > 1$, then we can have $m = n$. It is then possible for us to take $h := g^{-1}$, and we see this would make gh has order 1. This seems to be the point of question (b).*

Remark 3.6 (The more you know, the better)**.** *We have seen that when it comes to Problem (d), the problem becomes a bit non-trivial. We cannot simply use gh as our element for the proof. In fact, we can construct arbitrary order of gh for a group. For a nice proof, please refer to J.S. Mline's notes, starting at the bottom of page 28 (Link: https://www.jmilne.org/math/CourseNotes/GT.pdf). This also highlights the difficulty of group theory.*

□

Problem (5)**.** *Let G be a group. The center of G, denoted $Z(G)$, is the set of elements of G that commute with every other element. $Z(G) = \{g \in G : gh = hg$ for every h in $G\}$. (a) Prove that $Z(G)$ is a subgroup of G. (b) When does $Z(G)$ equal G? (Problem 2.35ab)*

Solution. For part (a) Let's recall the *Subgroup Test*: A set H in G is a subgroup whenever: $ab^{-1} \in H$ when $a, b \in H$. Let $z_1, z_2 \in Z(G)$ and $g \in G$. First note that if $z \in Z(G)$, then $z^{-1} \in Z(G)$. This is true since by hypothesis, for each $g \in G, zg = gz$, multiply both on the left and on the right by z^{-1}, which gives $z^{-1}zgz^{-1} = z^{-1}gzz^{-1}$ or more simply $gz^{-1} = z^{-1}g$. Now note that $z_1 z_2^{-1} g = z_1 g z_2^{-1} = g z_1 z_2^{-1}$, so $z_1 z_2^{-1} \in Z(G)$, and $Z(G)$ is a subgroup of G.

For part (b) if $Z(G) = G$, that means every element of G commutes with every element in G, so G is abelian. □

4 Homework 4

Due Date: Tuesday, October 14
Problems:

1. (Problem 3.5) We have already seen the ring of Gaussian integers $\mathbb{Z}[i]$. More generally, for any integer D that is not the square of an integer, we can form a ring

$$\mathbb{Z}[\sqrt{D}] \;=\; \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$

   If $D > 0$, then $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{R}$, while if $D < 0$, then in any case it is a subring of $\mathbb{C}$.

   (a) Let $\alpha = 2 + 3\sqrt{5}$ and $\beta = 1 - 2\sqrt{5}$ be elements of $\mathbb{Z}[\sqrt{5}]$. Compute the quantities

$$\alpha + \beta, \qquad \alpha \cdot \beta, \qquad \alpha^2$$

   (b) Prove that the map

$$\phi : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}], \quad \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

   is a ring homomorphism. (For notational convenience, if $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, then people often write $\bar{\alpha} = a - b\sqrt{D}$, similar to the notation for complex conjugation).

   (c) With the notation as in (b), prove that

$$\alpha \cdot \bar{\alpha} \in \mathbb{Z} \quad \text{for every } \alpha \in \mathbb{Z}[\sqrt{D}].$$

2. (Problem 3.6) Let $\rho = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ be the complex number, and let

$$\mathbb{Z}[\rho] \;=\; \{a + b\rho : a, b \in \mathbb{Z}\}.$$

   (a) Prove that $\rho^3 = 1$. Thus, ρ is a cube root of unity.

   (b) Prove that $\rho^2 + \rho + 1 = 0$. (*Hint.* This can be done by a direct calculation, but it's easier to use (a) and factor $\rho^3 - 1$.)

   (c) Prove that the polynomial $X^3 - 1$ factor as

$$X^3 - 1 = (X - 1)(X - \rho)(X - \rho^2).$$

   (d) Prove that $\mathbb{Z}[\rho]$ is a subring of $\mathbb{C}$. (The key here is to prove that if you add or multiply two elements of $\mathbb{Z}[\rho]$, you get back an element of $\mathbb{Z}[\rho]$.)

3. (Problem 3.7) Let $R = \mathbb{Z}/5\mathbb{Z}$, and let $f(x), g(x) \in R[x]$ be polynomials

$$f(x) \;=\; x^6 + 4x^5 + 4x^2 + 4x + 3 \qquad g(x) \;= x^6 + 3x^5 + 4x^2 + 3.$$

   Prove that

$$f(c) = g(c) \text{ for all } c \in R.$$

   Note that since the coefficients of $f(x)$ and $g(x)$ are not the same, we have $f(x) \neq g(x)$ in the ring $R[x]$, despite the fact that $f(x)$ and $g(x)$ define the same function $R \to R$.

4. (Problem 3.15a) Let R be a commutative ring, and let $f(x) \in R[x]$ be a polynomial with coefficients in R. We define the *formal derivative* $f'(x)$ of $f(x)$ by writing $f(x)$ as

$$f(x) \;=\; \sum_{k=0}^{n} a_k x^k \quad \text{and} \quad f'(x) \;=\; \sum_{k=1}^{n} k a_k x^{k-1}.$$

Note that there is no limit being taken, so the formal derivative makes sense even if, for example, R is a ring such as $\mathbb{Z}/m\mathbb{Z}$. It also means that when doing this exercise, you'll need to directly use the definition of $f'(x)$, since you can't rely on the proofs from calculus.

   (a) Let $f(x), g(x) \in R[x]$. Prove that $(f+g)'(x) = f'(x) + g'(x)$.

5. (Problem 3.17) Let R be a possibly *non-commutative* ring. The *center of* R consists of the elements of R that commute with every other element of R,

$$R^{\text{center}} \;=\; \{\alpha \in R : \alpha\beta = \beta\alpha \text{ for every } \beta \in R\}.$$

   (a) Prove that R^{center} is a commutative ring of R.

   (b) What is the center of the ring of quaternions $\mathbb{H}$?

   (c) Let F be a field. What is the center of the ring of 2-by-2 matrices $M_2(F)$ described in Example 3.8.

Solutions next page

Homework 4: Solutions

Problem (1)**.** *(Problem 3.5) We have already seen the ring of Gaussian integers $\mathbb{Z}[i]$. More generally, for any integer D that is not the square of an integer, we can form a ring*

$$\mathbb{Z}[\sqrt{D}] \;=\; \{a + b\sqrt{D} : a, b \in \mathbb{Z}\}.$$

If $D > 0$, then $\mathbb{Z}[\sqrt{D}]$ is a subring of $\mathbb{R}$, while if $D < 0$, then in any case it is a subring of $\mathbb{C}$.

(a) Let $\alpha = 2 + 3\sqrt{5}$ and $\beta = 1 - 2\sqrt{5}$ be elements of $\mathbb{Z}[\sqrt{5}]$. Compute the quantities

$$\alpha + \beta, \qquad \alpha \cdot \beta, \qquad \alpha^2$$

(b) Prove that the map

$$\phi : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}[\sqrt{D}], \quad \phi(a + b\sqrt{D}) = a - b\sqrt{D}$$

is a ring homomorphism. (For notational convenience, if $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, then people often write $\bar{\alpha} = a - b\sqrt{D}$, similar to the notation for complex conjugation).

(c) With the notation as in (b), prove that

$$\alpha \cdot \bar{\alpha} \in \mathbb{Z} \quad \textit{for every } \alpha \in \mathbb{Z}[\sqrt{D}].$$

Solution. For (a), we see by straightforward algebra that

$$\alpha + \beta \;=\; 3 + \sqrt{5} \qquad \alpha \cdot \beta \;=\; -28 - \sqrt{5} \qquad \alpha^2 \;=\; 49 + 12\sqrt{5}$$

For (b), we check if the map meets our condition for ring homomorphism following **Definition 3.3** from the textbook (page 65). We first see it meets condition (1), since

$$\phi(1_R) \;=\; \phi(1_R + 0\sqrt{D}) \;=\; 1_R - 0\sqrt{D} \;=\; 1_R.$$

We then show it meets condition (2). Consider arbitrary chosen elements $\alpha + \beta\sqrt{D}, a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, we then have

$$\begin{aligned}
\phi(a + b\sqrt{D} + \alpha + \beta\sqrt{D}) &= \phi\left((a + \alpha) + (b + \beta)\sqrt{D}\right) \\
&= (a + \alpha) - (b + \beta)\sqrt{D} \\
&= (a - b\sqrt{D}) + (\alpha - \beta\sqrt{D}) \\
&= \phi(a + b\sqrt{D}) + \phi(\alpha + \beta\sqrt{D}).
\end{aligned}$$

We then show it meets condition (3). First, we see

$$\begin{aligned}
\phi\left((a + b\sqrt{D}) \cdot (\alpha + \beta\sqrt{D}\right) &= \phi\left(a\alpha + b\beta D + a\beta\sqrt{D} + \alpha b\sqrt{D}\right) \\
&= (a\alpha + b\beta D) - (a\beta + \alpha b)\sqrt{D}.
\end{aligned}$$

Then, we see

$$\begin{aligned}\phi(a+b\sqrt{D})\cdot\phi(\alpha+\beta\sqrt{D}) &= (a-b\sqrt{D})\cdot(\alpha-\beta\sqrt{D})\\ &= a\alpha - a\beta\sqrt{D} - \alpha b\sqrt{D} + b\beta D\\ &= (a\alpha + b\beta D) - (a\beta + b\alpha)\sqrt{D}.\end{aligned}$$

We see the left hand side and the right hand side are indeed equal, proving the desired claim.

For (c), consider $a+b\sqrt{D}, a-b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. We see that

$$\begin{aligned}(a+b\sqrt{D})\cdot(a-b\sqrt{D}) &= a(a-b\sqrt{D}) + b\sqrt{D}(a-b\sqrt{D})\\ &= a^2 - ab\sqrt{D} + ab\sqrt{D} - b^2D\\ &= a^2 - b^2D \in \mathbb{Z},\end{aligned}$$

proving the desired claim. □

Problem (2). *(Problem 3.6) Let $\rho = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ be the complex number, and let*

$$\mathbb{Z}[\rho] \;=\; \{a+b\rho : a,b \in \mathbb{Z}\}.$$

(a) Prove that $\rho^3 = 1$. Thus, ρ is a cube root of unity.

(b) Prove that $\rho^2 + \rho + 1 = 0$. (Hint. This can be done by a direct calculation, but it's easier to use (a) and factor $\rho^3 - 1$.)

(c) Prove that the polynomial $X^3 - 1$ factor as

$$X^3 - 1 = (X-1)(X-\rho)(X-\rho^2).$$

(d) Prove that $\mathbb{Z}[\rho]$ is a subring of $\mathbb{C}$. (The key here is to prove that if you add or multiply two elements of $\mathbb{Z}[\rho]$, you get back an element of $\mathbb{Z}[\rho]$.)

Solution. For (a), we see that

$$\begin{aligned}\left(\frac{-1+i\sqrt{3}}{2}\right)^3 &= \left(\frac{1}{2}(-1+i\sqrt{3})\right)^3\\ &= \frac{1}{8}(-1+i\sqrt{3})^3\\ &= \frac{1}{8}\left((-1)^3 + 3(-1)^2 i\sqrt{3} + 3(-1)(i\sqrt{3})^2 + (i\sqrt{3})^3\right)\\ &= \frac{1}{8}\left(-1 + 3i\sqrt{3} + 9 - 3i\sqrt{3}\right)\\ &= 1.\end{aligned}$$

A more illuminating way is to observe that on the unit circle, we have

$$e^{2\pi i/3} \;=\; \frac{-1+i\sqrt{3}}{2} \Longrightarrow (e^{2\pi i/3})^3 \;=\; 1.$$

For (b), we shall use previous result. We already see that $\rho^3 - 1 = 0$ from (a). Now, observe that if we consider

$$\begin{aligned}\rho^3 - 1 &= \rho^3 + \rho^2 + \rho - \rho^2 - \rho - 1 \\ &= (\rho - 1)(\rho^2 + \rho + 1).\end{aligned}$$

We see that $\rho \neq 0$ by definition, so $\rho - 1 \neq 0$. Thus, we must have $\rho^2 + \rho + 1 = 0$ as desired.
Alternatively, one can use simple brute force calculation to show the above result. We have

$$\begin{aligned}\rho^2 + \rho + 1 &= \left(\frac{-1+i\sqrt{3}}{2}\right)^2 + \frac{-1+i\sqrt{3}}{2} + 1 \\ &= \frac{1 - 2i\sqrt{3} - 3}{4} + \frac{-1+i\sqrt{3}}{2} + 1 \\ &= 0.\end{aligned}$$

For (c), we see by straightforward computation that

$$\begin{aligned}(X-1)(X-\rho)(X-\rho^2) &= X^3 - X^2\rho - X^2\rho^2 + X\rho^3 - X^2 + X\rho^2 + X\rho - \rho^3 \\ &= X^3 - X^2(\rho^2 + \rho + 1) + X(\rho^2 + \rho + 1) - \rho^3 \\ &= X^3 - \rho^3 \\ &= X^3 - 1,\end{aligned}$$

where we have used the facts from (a) and (b) that $\rho^3 = 1$ and $\rho^2 + \rho + 1 = 0$, respectively.

For (d), we shall prove that $\mathbb{Z}[\rho]$ is a subring of $\mathbb{C}$. It is clear that $\mathbb{Z}[\rho] \subsetneq \mathbb{C}$ from its definition. We first check it is closed under addition. Consider $a + b\rho, \alpha + \beta\rho \in \mathbb{Z}[\rho]$, we then have

$$(a + b\rho) + (\alpha + \beta\rho) = (a + \alpha) + (b + \beta)\rho \in \mathbb{Z}[\rho].$$

We then show it is closed under multiplication. By simple algebra, we have

$$\begin{aligned}(a + b\rho) \cdot (\alpha + \beta\rho) &= a(\alpha + \beta\rho) + b\rho(\alpha + \beta\rho) \\ &= a\alpha + a\beta\rho + \alpha b\rho + \beta b\rho^2 \\ &= a\alpha + a\beta\rho + \alpha b\rho + \beta b(-\rho - 1) \\ &= a\alpha + a\beta\rho + \alpha b\rho - \beta b\rho - \beta b \\ &= a\alpha - \beta b + (a\beta + \alpha b - \beta b)\rho \in \mathbb{Z}[\rho],\end{aligned}$$

where we have recalled the fact that $\rho^2 = -\rho - 1$ from question (b). This is sufficient for showing that $\mathbb{Z}[\rho]$ is indeed a subring of $\mathbb{C}$.

Remark 4.1. *Question. Why showing closure under addition and multiplication suffices for proving $\mathbb{Z}[\rho]$ is a subring of $\mathbb{C}$?*

□

Problem (3)**.** *(Problem 3.7) Let $R = \mathbb{Z}/5\mathbb{Z}$, and let $f(x), g(x) \in R[x]$ be polynomials*

$$f(x) \ = \ x^6 + 4x^5 + 4x^2 + 4x + 3 \qquad g(x) \ = x^6 + 3x^5 + 4x^2 + 3.$$

Prove that

$$f(c) = g(c) \text{ for all } c \in R.$$

Note that since the coefficients of $f(x)$ and $g(x)$ are not the same, we have $f(x) \neq g(x)$ in the ring $R[x]$, despite the fact that $f(x)$ and $g(x)$ define the same function $R \to R$.

Solution. We can verify the above result by straightforward computation. For $f(x)$, we have

$$\begin{aligned} f(0) &= 0^6 + 4 \cdot 0^5 + 4 \cdot 0^2 + 4 \cdot 0 + 3 = 3 \\ f(1) &= 1^6 + 4 \cdot 1^5 + 4 \cdot 1^2 + 4 \cdot 1 + 3 = 1 \\ f(2) &= 2^6 + 4 \cdot 2^5 + 4 \cdot 2^2 + 4 \cdot 2 + 3 = 4 \\ f(3) &= 3^6 + 4 \cdot 3^5 + 4 \cdot 3^2 + 4 \cdot 3 + 3 = 2 \\ f(4) &= 4^6 + 4 \cdot 4^5 + 4 \cdot 4^2 + 4 \cdot 4 + 3 = 0 \end{aligned}$$

For $g(x)$, we have

$$\begin{aligned} g(0) &= 0^6 + 3 \cdot 0^5 + 4 \cdot 0^2 + 3 = 3 \\ g(1) &= 1^6 + 3 \cdot 1^5 + 4 \cdot 1^2 + 3 = 1 \\ g(2) &= 2^6 + 3 \cdot 2^5 + 4 \cdot 2^2 + 3 = 4 \\ g(3) &= 3^6 + 3 \cdot 3^5 + 4 \cdot 3^2 + 3 = 2 \\ g(4) &= 4^6 + 3 \cdot 4^5 + 4 \cdot 4^2 + 3 = 0 \end{aligned}$$

We indeed see that $f(c) = g(c)$ for all $c \in R$. This way seems so inefficient. What if we have $R = \mathbb{Z}/p\mathbb{Z}$ for some sufficiently large prime p, then brute force would not work anymore. But observe that we have

$$f(x) - g(x) = x^5 + 4x = x^5 - x$$

Observe that by Fermat's Little Theorem, we indeed have $f(c) - g(c) = 0$ for all $c \in R$, giving us the desired result.

Remark 4.2. *Observe that something interesting is happening above. We see that $f(x)$ and $g(x)$ have different coefficients, but $f(c) = g(c)$ for all $c \in R$. We can therefore say they give the exact same mapping from R to R. This seems to be true for this reasonably nice finite ring R, but what if we have an infinite ring R? That*

is, given a "reasonably nice" infinite ring R, what can we say about $f(x), g(x)$ if we have $f(c) = g(c)$ for all elements $c \in R$?

□

Problem (4)**.** *(Problem 3.15a) Let R be a commutative ring, and let $f(x) \in R[x]$ be a polynomial with coefficients in R. We define the formal derivative $f'(x)$ of $f(x)$ by writing $f(x)$ as*

$$f(x) \;=\; \sum_{k=0}^{n} a_k x^k \quad \textit{and} \quad f'(x) \;=\; \sum_{k=1}^{n} k a_k x^{k-1}.$$

Note that there is no limit being taken, so the formal derivative makes sense even if, for example, R is a ring such as $\mathbb{Z}/m\mathbb{Z}$. It also means that when doing this exercise, you'll need to directly use the definition of $f'(x)$, since you can't rely on the proofs from calculus.

(a) Let $f(x), g(x) \in R[x]$. Prove that $(f+g)'(x) = f'(x) + g'(x)$.

Solution. Define $f(x), g(x) \in R[x]$ such that

$$f(x) = \sum_{k=0}^{n} a_k x^k \qquad g(x) = \sum_{k=1}^{m} b_k x^k$$

Let $N := \max(n, m)$ and we make the coefficients identically zero if it is out of index. This then gives

$$\begin{aligned}
(f+g)'(x) &= \sum_{k=0}^{N} k(a_k + b_k) x^{k-1} \\
&= \sum_{k=1}^{N} k a_k x^{k-1} + \sum_{k=1}^{N} k b_k x^{k-1} \\
&= \sum_{k=1}^{n} k a_k x^{k-1} + \sum_{k=1}^{m} k b_k x^{k-1} \\
&= f'(x) + g'(x)
\end{aligned}$$

Remark 4.3. *There is a reason that we say the above definition is formal. It is that it does not behave like our derivative defined in calculus class. Consider $f(x) = x^2 + x$ over $\mathbb{Z}/2\mathbb{Z}$. We indeed see that*

$$f(0) = 0 \qquad f(1) = 0,$$

and we know the derivative is given by $f'(x) = 2x + 1$. We see that

$$f'(0) = 1 \qquad f(1) = 1.$$

□

Problem (5)**.** *(Problem 3.17) Let R be a possibly non-commutative ring. The center of R consists of the elements of R that commute with every other element of R,*

$$R^{\textit{center}} \;=\; \{\alpha \in R : \alpha\beta = \beta\alpha \textit{ for every } \beta \in R\}.$$

(a) Prove that R^{center} is a commutative ring of R.

(b) What is the center of the ring of quaternions $\mathbb{H}$?

(c) Let F be a field. What is the center of the ring of 2-by-2 matrices $M_2(F)$ described in Example 3.8.

Solution. For (a), we show R^{center} meets the definition of a commutative ring. It is straightforward to see that

$$0_R, 1_R \in R^{\text{center}},$$

since we have

$$0_R \cdot \alpha = \alpha \cdot 0_R = 0_R \qquad 1_R \cdot \alpha = \alpha \cdot 1_R = \alpha$$

by definition. We first show R^{center} is a subring of R by checking it is closed under addition and multiplication. Consider $\alpha, \beta \in R^{\text{center}}$ and $\gamma \in R$. We then have

$$\begin{aligned}(\alpha + \beta) \cdot \gamma &= \alpha \cdot \gamma + \beta \cdot \gamma \\ &= \gamma \cdot \alpha + \gamma \cdot \beta \\ &= \gamma \cdot (\alpha + \beta),\end{aligned}$$

so we see $\alpha + \beta \in R^{\text{center}}$. We then show it is closed under multiplication. We have

$$\begin{aligned}(\alpha \cdot \beta) \cdot \gamma &= \alpha \cdot (\beta \cdot \gamma) \\ &= \alpha \cdot (\gamma \cdot \beta) \\ &= (\alpha \cdot \gamma) \cdot \beta \\ &= (\gamma \cdot \alpha) \cdot \beta \\ &= \gamma \cdot (\alpha \cdot \beta),\end{aligned}$$

so we see $\alpha \cdot \beta \in R^{\text{center}}$. This concludes that it is a subring of R. Last, we simply observe that every element of R^{center} commutes with any element in R, and $R^{\text{center}} \subseteq R$, proving that it is indeed a commutative ring.

For (b), we see that the center of the ring of $\mathbb{H}$ is given by $\mathbb{R}$. To see this, we suppose $a+bi+cj+dk \in R^{\text{center}}$. By definition of R^{center}, we must have

$$i(a + bi + cj + dk) = (a + bi + cj + dk)i,$$

and we see this gives

$$i(a + bi + cj + dk) = ai - b + ck - dj \qquad (a + bi + cj + dk)i = ai - b - ck + dj.$$

For the equality to hold, we need $c = d = 0$. Similarly, we must have

$$j(a + bi + cj + dk) = (a + bi + cj + dk)j,$$

and we need $b = 0$ for the equality to hold. This then means $a + bi + cj + dk \in R^{\text{center}}$ if and only if $b = c = d = 0$. We know $a \in \mathbb{R}$, so this means $\mathbb{R} = R^{\text{center}}$.

For (c), we first observe that the identity matrix I is in R^{center} as well as any multiples of it. The interesting question is whether there exists other elements in R^{center}. We suppose

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{\text{center}}.$$

such that it is not equal to aI for $a \in F$.
It is sufficient to consider the behavior of the center element with some simple matrices in $M_2(F)$. We must then have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Performing algebra, we see that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

and we need $c = b = 0$ for the equality to hold.
We also need the equality

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

to hold. But we see this gives

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix},$$

and we need $a = d$ and $c = 0$ for the equality to hold. Summing up previous results, we see that this implies the center element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ must be in the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, proving that

$$R^{\text{center}} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : \text{ for } a \in F \right\}.$$

□

5 Homework 5

Due Date: November 4, 2025
Problems:

1. (Problem 3.24) Let R be a commutative ring. The *degree* of non-zero polynomial $f(x) \in R[x]$ is the highest power of x that appears in $f(x)$. Thus, $f(x)$ has degree d if $f(x)$ has the form

$$f(x) \;=\; a_0 + a_1 x + \cdots + a_d x^d \quad \text{with } a_0, \ldots, a_d \in R \text{ and } a_d \neq 0.$$

   (a) Prove that for all $f(x), g(x) \in R[x]$, we have

$$\deg\left(f(x) + g(x)\right) \leq \max\left\{\deg(f(x)), \deg(g(x))\right\}.$$

   (b) If $f(x) \neq g(x)$, show that (a) is an equality.

   (c) Suppose that R is an integral domain, *i.e., assume that R has no zero divisors*. Prove that for all non-zero $f(x), g(x) \in R[x]$, we have

$$\deg\left(f(x)g(x)\right) = \deg(f(x)) + \deg(g(x)).$$

   (d) Let $R = \mathbb{Z}/6\mathbb{Z}$. Find polynomials $f(x), g(x) \in R[x]$ with $\deg\left(f(x)\right) = 1$ and $\deg\left(g(x)\right) = 1$ such that the equation in (c) is not an equality.

2. (Problem 3.25 ab) Let R be a commutative ring.

   (a) Prove that there is exactly one integral domain R such that the map

$$f : R \to R, \quad f(a) = a^6$$

   is a ring homomorphism (You'll use the fact that $1_R \neq 0_R$).

   (b) Find at least two different integral domains R such that the map

$$f : R \to R, \quad f(a) = a^{15}$$

   is a ring homomorphism. Are there any others?

3. (Problem 3.25 c)

   (a) For each of parts (a) and (b), find at least one ring that is not an integral domain for which the indicated map is a ring homomorphism.

4. (Problem 3.30 a) Compute the unit group $(\mathbb{Z}/p\mathbb{Z})^*$ for each of the primes $p = 7; 11; 13$. Which ones are cyclic?

5. (Problem 3.30 b) Compute the unit group $(\mathbb{Z}/m\mathbb{Z})^*$ for each of the composite numbers $m = 8; 9; 15$. Which ones are cyclic?

6. (Problem 3.47) Let R be a commutative ring, and let I be an ideal of R. For $a \in R$, we will denote the coset $a + I$ by $\bar{a}$; *i.e.*,

$$R \to R/I, \qquad a \to \bar{a},$$

is the reduction modulo I homomorphism. We define a map of polynomial rings

$$\phi : R[x] \to (R/I)[x], \qquad \phi(a_0 + a_1x + a_2x^2 + \cdots + a_dx^d) \;=\; \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \cdots + \bar{a}_dx^d,$$

by reducing the coefficients modulo I. Prove that ϕ is a ring homomorphism.

7. (Problem 3.48) Let R be a commutative ring and let I and J be ideals of R

   (a) Prove that the intersection $I \cap J$ is an ideal of R.

   (b) Prove that the *ideal sum*

   $$I + J \;=\; \{a + b : a \in I \text{ and } b \in J\}$$

   is an ideal of R.

   (c) The *ideal product* of two ideals is defined to be

   $$IJ \;=\; \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : n \geq 1 \text{ and } a_1, \cdots, a_n \in I \text{ and } b_1, \cdots, b_n \in J\}$$

   Prove that IJ is an ideal of R.

   (d) One might ask why the product IJ of ideals isn't simply defined as the set of products $\{ab : a \in I \text{ and } b \in J\}$. The answer is that the set of products need not be an ideal. Here is an example. Let $R = \mathbb{Z}[x]$, and let I and J be ideals

   $$I \;=\; 2\mathbb{Z}[x] + x\mathbb{Z}[x] \qquad J \;=\; 3\mathbb{Z}[x] + x\mathbb{Z}[x]$$

   Prove that the set of products $\{ab : a \in I \text{ and } b \in J\}$ is not an ideal.

   (e) On the other hand, prove in general that if either I or J is a principal ideal, then the set of products $\{ab : a \in I \text{ and } b \in J\}$.

8. (Problem 3.51) Let I be the following subset of the ring $\mathbb{Z}[x]$ of polynomials having integer coefficients:

   $$I \;=\; \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\}.$$

   (a) Prove that I is an ideal of $\mathbb{Z}[x]$.

   (b) Prove that $I \neq \mathbb{Z}[x]$.

   (c) Prove that I is not a principal ideal, *i.e.*, prove that there does not exist a polynomial $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$.

   (d) Prove that I is a maximal ideal of $\mathbb{Z}[x]$.

Solutions next page

Homework 5: Solutions

Problem (1). *(Problem 3.24) Let R be a commutative ring. The* degree *of non-zero polynomial $f(x) \in R[x]$ is the highest power of x that appears in $f(x)$. Thus, $f(x)$ has degree d if $f(x)$ has the form*

$$f(x) \;=\; a_0 + a_1 x + \cdots + a_d x^d \quad \textit{with } a_0, \ldots, a_d \in R \textit{ and } a_d \neq 0.$$

(a) Prove that for all $f(x), g(x) \in R[x]$, we have

$$\deg\left(f(x) + g(x)\right) \leq \max\left\{\deg(f), \deg(g)\right\}.$$

(b) If $\deg(f) \neq \deg(g)$, show that (a) is an equality.

(c) Suppose that R is an integral domain, i.e., assume that R has no zero divisors. *Prove that for all non-zero $f(x), g(x) \in R[x]$, we have*

$$\deg\left(f(x)g(x)\right) = \deg(f) + \deg(g).$$

(d) Let $R = \mathbb{Z}/6\mathbb{Z}$. Find polynomials $f(x), g(x) \in R[x]$ with $\deg\left(f(x)\right) = 1$ and $\deg\left(g(x)\right) = 1$ such that the equation in (c) is not an equality.

Solution. For (a), we consider $f(x), g(x) \in R[x]$ such that

$$f(x) \;=\; a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad g(x) \;=\; b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

with $\deg(f) = n$ and $\deg(g) = m$. Without loss of generality, we consider $n \geq m$. If $n > m$, we then have

$$f(x) + g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 + b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

It is then clear that $\deg(f+g) = \max\{\deg(f), \deg(g)\}$, where the maximum is given by $\deg(f) = n$. If $n = m$, we then have

$$\begin{cases} f(x) + g(x) = (a_n + b_m)x^n + a_{n-1}x^{n-1} + b_{m-1}x^{m-1} \cdots + (a_0 + b_0), \text{ if } a_n \neq -b_m \\ f(x) + g(x) = 0 \cdot x^n + a_{n-1}x^{n-1} + b_{m-1}x^{m-1} + \cdots + (a_0 + b_0) \qquad \text{, if } a_n = -b_m \end{cases}$$

In the first case, we see that we obtain $\deg(f+g) = \max\{\deg(f), \deg(g)\}$, since the highest power x^n in $(f+g)(x)$ has non-zero coefficient. In the second case, we see that $\deg(f+g) < \max\{\deg(f), \deg(g)\}$, since the highest power x^n in $(f+g)(x)$ vanishes. This completes the proof.

For (b), observe that the assumption $\deg(f) \neq \deg(g)$ implies $\deg(f) > \deg(g)$ or $\deg(f) < \deg(g)$. This equality is already proved in (a), as the highest degree monomial cannot be cancelled out by hypothesis, and thus the claim must hold.

Remark 5.1. *Notice in the proof all we need to rely on is that the highest degree term does not cancel out. Therefore we can weaken the hypothesis here slightly. If we denote the leading term of a polynomial as* $\mathrm{LT}(f)$*, then equality holds in part (a) as long as* $\mathrm{LT}(f) \neq -\mathrm{LT}(g)$

For (c), we study $f(x)$ and $g(x)$ found in (a). After expansion, we see that

$$\begin{aligned} f(x)g(x) &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \cdot (b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0) \\ &= a_n b_m x^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0 \end{aligned}$$

We know that a_n, b_m are non-zero by assumption and we are guaranteed that $a_n \cdot b_m \neq 0$, since R is an integral domain. We see $\deg(f(x)g(x)) = n + m$, where $\deg(f) = n$ and $\deg(g) = m$, proving the desired equality.

For (d), we simply consider $f(x) = 2x$ and $g(x) = 3x$ for $f(x), g(x) \in (\mathbb{Z}/6\mathbb{Z})[x]$. We see $\deg(f) = \deg(g) = 1$, but $f(x)g(x) = 6x^2 = 0$ in $\mathbb{Z}/6\mathbb{Z}$. Thus, $\deg(f(x)g(x)) \neq \deg(f) + \deg(g)$ □

Problem (2)**.** *(Problem 3.25 ab) Let R be a commutative ring.*

(a) Prove that there is exactly one integral domain R such that the map

$$f : R \to R, \quad f(a) = a^6$$

is a ring homomorphism (You'll use the fact that $1_R \neq 0_R$).

(b) Find at least two different integral domains R such that the map

$$f : R \to R, \quad f(a) = a^{15}$$

is a ring homomorphism. Are there any others?

Solution. For (a), we first consider the characteristic of ring R determined by $f(a) = a^6$. We first observe that

$$f(1+1) = 2^6 = 32 \qquad \text{and} \qquad f(1) + f(1) = 2.$$

Since f is a ring homomorphism, we have $f(1+1) = f(1) + f(1)$; this immediately implies we have $32 = 2$ or $30 = 0$ in R. Next, we observe that

$$f(1+2) = (1+2)^6 = 729 \qquad \text{and} \qquad f(1) + f(2) = 1^6 + 2^6 = 65.$$

This gives $729 = 65$ or $664 = 0$ in R. We are trying to determine the characteristic of R, so we have

$$\gcd(664, 30) = 2.$$

Consider arbitrary elements $a, b \in R$. By simple expansion, we have

$$\begin{aligned} f(a+b) &= (a+b)^6 \\ &= a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\ &= a^6 + b^6 + (6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5), \end{aligned}$$

where we see the last term is 0 by the fact that $f(a+b) = f(a) + f(b)$. Since R has characteristic of 2, we then must have

$$6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 = a^4b^2 + a^2b^4 = a^2b^2(a^2 + b^2).$$

Observe that we want R to be an integral domain, so we have $ab \neq 0$ for non-zero $a, b \in R$. This then implies $a^2 + b^2 = 0$. We further observe that

$$a^2 + 2ab + b^2 = (a+b)^2 = 0,$$

so we must have $a + b = 0$ for all non-zero $a, b \in R$. Since $2 = 0$ in R, we must then have $a = -b = 1$. This then gives $R = \{0, 1\}$ or $\mathbb{Z}/2\mathbb{Z}$.

For (b), we replicate the idea used in (a). We observe that

$$f(1+1) \;=\; 2^{15} \qquad \text{and} \qquad f(1) + f(1) = 2.$$

Furthermore, we see that

$$f(1+1+1) \;=\; 3^{15} \qquad \text{and} \qquad f(1) + f(1) + f(1) = 3.$$

By the that $f(a+b) = f(a) + f(b)$, we observe that

$$0 \;=\; 2^{15} - 2 \;=\; 32766 \qquad\qquad 0 \;=\; 3^{15} - 3 \;=\; 14348904.$$

We find that the characteristic of the ring is given by $\gcd(32766, 14348904) = 6$. But observe that $6 = 2{\cdot}3 \equiv 0$, so we either have $2 \equiv 0$ or $3 \equiv 0$. We see that $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ would work here.

□

Problem (3)**.** *(Problem 3.25 c)*

1. *For each of parts (a) and (b), find at least one ring that is not an integral domain for which the indicated map is a ring homomorphism.*

Solution. For (c), one can try $\mathbb{Z}/6\mathbb{Z}$ and verify that this is indeed a ring homomorphism in both cases.

Remark 5.2. *For (a), once we have deduced that $\mathbb{Z}/2\mathbb{Z}$ satisfies the map $f(a) = a^6$, this already implies that we have exactly one integral satisfying such map. This is because we know that the only Boolean ring that is an integral domain is $\mathbb{Z}/2\mathbb{Z}$. This can be proved by considering $a^2 - a = a(a-1) = 0$.*

□

Problem (4)**.** *(Problem 3.30 a) Compute the unit group $(\mathbb{Z}/p\mathbb{Z})^*$ for each of the primes $p = 7; 11; 13$. Which ones are cyclic?*

Solution. They are all cyclic. By simple computation, we see that the unit groups are given by

$$\begin{aligned}\mathbb{Z}/7\mathbb{Z} &= \{1, 2, 3, 4, 5, 6\} \\ \mathbb{Z}/11\mathbb{Z} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \\ \mathbb{Z}/13\mathbb{Z} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.\end{aligned}$$

One can verify that 3 is a generator for $\mathbb{Z}/7\mathbb{Z}$, 2 is a generator for $\mathbb{Z}/11\mathbb{Z}$, and 2 is a generator for $\mathbb{Z}/13\mathbb{Z}$.

Remark 5.3. *In fact, we know that if F is a field, then any finite subgroup of F^* is indeed cyclic.*

□

Problem (5)**.** *(Problem 3.30 b) Compute the unit group $(\mathbb{Z}/m\mathbb{Z})^*$ for each of the composite numbers $m = 8; 9; 15$. Which ones are cyclic?*

Solution. By simple computation, one can see that the unit groups are the set of all positive integers that are coprime with m, which gives the following:

$$\begin{aligned}\mathbb{Z}/8\mathbb{Z} &= \{1, 3, 5, 7\}\\ \mathbb{Z}/9\mathbb{Z} &= \{1, 2, 4, 5, 7, 8\}\\ \mathbb{Z}/15\mathbb{Z} &= \{1, 2, 4, 7, 8, 11, 13, 14\}.\end{aligned}$$

We see that only $m = 9$ is cyclic in this case. □

Problem (6)**.** *(Problem 3.47) Let R be a commutative ring, and let I be an ideal of R. For $a \in R$, we will denote the coset $a + I$ by $\bar{a}$;* i.e.*,*

$$R \to R/I, \qquad a \to \bar{a},$$

is the reduction modulo I homomorphism. We define a map of polynomial rings

$$\phi : R[x] \to (R/I)[x], \qquad \phi(a_0 + a_1x + a_2x^2 + \cdots + a_dx^d) \;=\; \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \cdots + \bar{a}_dx^d,$$

by reducing the coefficients modulo I. Prove that ϕ is a ring homomorphism.

Solution. We can easily see that $\phi(0) = \overline{0}$ and $\phi(1) = \overline{1}$. Without loss of generality, we argue it suffices to consider polynomials of the same degree d

$$f(x) \;=\; \sum_{i=0}^{d} a_ix^i \in R[x] \qquad \text{and} \qquad g(x) \;=\; \sum_{i=0}^{d} b_ix^i \in R[x],$$

where we allow some some a_i or b_i to vanish to preserve generality.

We first check $\phi(a+b) = \phi(a) + \phi(b)$. We have

$$\begin{aligned}
\phi\left(f(x)+g(x)\right) &= \phi\left(\sum_{i=0}^{d} a_i x^i + \sum_{i=0}^{d} b_i x^i\right) \\
&= \phi\left(\sum_{i=0}^{d} (a_i + b_i) x^i\right) \\
&= \sum_{i=0}^{d} \overline{(a_i + b_i)} x^i \\
&= \sum_{i=0}^{d} (\overline{a_i} + \overline{b_i}) x^i \qquad \text{since } a \to \overline{a} \text{ is a homomorphism} \\
&= \sum_{i=0}^{d} \overline{a_i} x^i + \sum_{i=0}^{d} \overline{b_i} x^i \\
&= \phi(f(x)) + \phi(g(x))
\end{aligned}$$

We then check $\phi(ab) = \phi(a)\phi(b)$. We have

$$\begin{aligned}
\phi\left(f(x)g(x)\right) &= \phi\left(\left(\sum_{i=0}^{d} a_i x^i\right) \cdot \left(\sum_{j=0}^{d} b_i x^i\right)\right) \\
&= \phi\left(\sum_{i=0}^{d} \sum_{j=0}^{d} a_i b_j x^{i+j}\right) \\
&= \sum_{i=0}^{d} \sum_{j=0}^{d} \phi\left(a_i b_j x^{i+j}\right) \text{ we know } \phi(a+b) = \phi(a) + \phi(b) \\
&= \sum_{i=0}^{d} \sum_{j=0}^{d} \overline{a_i \cdot b_j} x^{i+j} \\
&= \sum_{i=0}^{d} \sum_{j=0}^{d} \overline{a_i} \cdot \overline{b_j} x^{i+j} \\
&= \sum_{i=0}^{d} \overline{a_i} x^i \cdot \sum_{j=0}^{d} \overline{b_j} x^j \\
&= \phi(f(x)) \cdot \phi(g(x))
\end{aligned}$$

This completes the proof that $\phi : R[x] \to (R/I)[x]$ is a homomorphism. □

Problem (7)**.** *(Problem 3.48) Let R be a commutative ring and let I and J be ideals of R*

(a) Prove that the intersection $I \cap J$ is an ideal of R.

(b) Prove that the ideal sum

$$I + J \;=\; \{a + b : a \in I \textit{ and } b \in J\}$$

is an ideal of R.

(c) The ideal product *of two ideals is defined to be*

$$IJ \;=\; \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : n \geq 1 \textit{ and } a_1, \cdots, a_n \in I \textit{ and } b_1, \cdots, b_n \in J\}$$

Prove that IJ is an ideal of R.

(d) One might ask why the product IJ of ideals isn't simply defined as the set of products $\{ab : a \in I \textit{ and } b \in J\}$. The answer is that the set of products need not be an ideal. Here is an example. Let $R = \mathbb{Z}[x]$, and let I and J be ideals

$$I \;=\; 2\mathbb{Z}[x] + x\mathbb{Z}[x] \qquad J \;=\; 3\mathbb{Z}[x] + x\mathbb{Z}[x]$$

Prove that the set of products $\{ab : a \in I \textit{ and } b \in J\}$ is not an ideal.

(e) On the other hand, prove in general that if either I or J is a principal ideal, then the set of products $\{ab : a \in I \textit{ and } b \in J\}$.

Solution. For part (a), we show that $I \cap J$ is an ideal of R. We first show that if $a \in I$ and $r \in R$, then $ra \in I$. Let $a \in I \cap J$ and $r \in R$. By definition of intersection, we then see that $a \in I$, so $ra \in I$ and similarly $a \in J$, so $ra \in J$. Hence, $ra \in I \cap J$.
We then show if $a \in I$ and $b \in I$, then $a + b \in I$. Consider arbitrary chosen elements $a, b \in I \cap J$. By definition of intersection, we then see $a \in I$ and $b \in I$, so $a + b \in I$, and $a \in J$ and $b \in J$, so $a + b \in J$, Hence, $a + b \in I \cap J$. This proves that $I \cap J$ is an ideal.

For (b), we show that $I + J$ is an ideal of R, following procedure similar to (a). We first show that if $a \in I + J$ and $r \in R$, then $ra \in I + J$. Indeed, consider $a + b \in I + J$, where $a \in I$ and $b \in J$, and let $r \in R$. Then $a \in I$, so $ra \in I$, and similarly $b \in J$, so $rb \in J$. Hence $ra + rb = r(a + b) \in I + J$.
Next, we show if $a, b \in I + J$, then $a + b \in I + J$. Consider $a_1 + b_1, a_2 + b_2 \in I + J$, where $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then, $a_1 + a_2 \in I$ and $b_1 + b_2 \in J$, so we have

$$(a_1 + b_1) + (a_2 + b_2) = (a_1 + a_2) + (b_1 + b_2) \in I + J.$$

This completes that $I + J$ is an ideal.

For (c), this is still checking the definition, though it is a bit more invovled. Let $a_1b_1 + \cdots + a_nb_n \in IJ$ and $r \in R$. Then

$$r(a_1b_1 + \cdots + a_nb_n) \;=\; ra_1b_1 + \cdots + ra_nb_n \;=\; (ra_1)b_1 + \cdots + (ra_n)b_n \in IJ,$$

since we know $ra_1, \ldots, ra_n \in I$.
We then consider $a_1b_1 + \cdots + a_nb_n \in IJ$ and $a_1'b_1' + \cdots + a_n'b_n' \in IJ$. Then,

$$(a_1b_1 + \cdots + a_nb_n) + (a_1'b_1' + \cdots + a_n'b_n') = a_1b_1 + \cdots + a_nb_n + a_1'b_1' + \cdots + a_n'b_n' \in IJ,$$

since it is a sum following the definition of the set. This proves that IJ is an ideal.

For (d), it suffices to find a polynomial that we cannot express in terms of I and J. Define the set of products as

$$\mathcal{S} = \{f(x)g(x) : f(x) \in I \quad \text{and} \quad g(x) \in J\}.$$

Then, simply consider $\alpha, \beta \in \mathcal{S}$ such that

$$\alpha \ = \ (2+x)(3+x) \qquad\qquad \beta \ = \ (4+x)(6+x).$$

We then have

$$\begin{aligned}\alpha + \beta &= (2+x)(3+x) + (4+x)(6+x) \\ &= x^2 + 5x + 6 + x^2 + 10x + 24 \\ &= 2x^2 + 15x + 30.\end{aligned}$$

We claim $\alpha + \beta \notin \mathcal{S}$, thus showing it is not an ideal. To this end, we have to show that there does not exist $f(x) \in I, g(x) \in J$ such that $f(x)g(x) = 2x^2 + 15x + 30$.
We suppose for the contrary that there exist $f(x) \in I, g(x) \in J$ such that the above decomposition is possible. By studying the parity of the coefficients of the polynomial above, we see that $f(x)$ and $g(x)$ cannot be constant. For example, if $f(x)$ were a constant, then it has to be even by definition of I. We know this would imply the coefficients of $\alpha + \beta$ to be all even, since the product of an even number with any integer is always even, but 15 is odd. A similar argument can be used for $g(x)$. We thus know $f(x)$ and $g(x)$ are non-constant polynomials.
Since $\alpha + \beta$ is degree 2, we see $f(x), g(x)$ have to be degree 1, and we have

$$\alpha + \beta \ = \ 2x^2 + 15x + 30 \ = \ (a_0 + a_1 x)(b_0 + b_1 x)$$

for $a_0, a_1, b_0, b_1 \in \mathbb{Z}$. We know $-\frac{a_0}{a_1}, -\frac{b_0}{b_1}$ have to be the roots of $\alpha + \beta$, but we see the roots of $\alpha + \beta$ are given by

$$\frac{-15 \pm \sqrt{-15}}{4} \notin \mathbb{R}$$

by the quadratic formula. This gives the desired contradiction, proving that $\alpha + \beta \notin \mathcal{S}$.

For (e), we define $\mathcal{S} = \{ab : a \in I, b \in J\}$ be the set of products. Without loss of generality, we assume that I is principal and we want to show that $\mathcal{S}$ is an ideal. Suppose we have $a_0 \in I$ and let $b_1, b_2 \in J$, so we have that $a_0 b_1$ and $a_0 b_2$ are in $\mathcal{S}$. Then their sum is

$$a_0 b_1 + a_0 b_2 = a_0(b_1 + b_2) \in \mathcal{S},$$

since the fact that J is an ideal tells us that $b_1 + b_2 \in J$. Similarly, if $r \in R$, then for any $ab \in \mathcal{S}$ we have $rab = (ra)b \in \mathcal{S}$, since the fact that I is an ideal tells us that $ra \in I$.

Remark 5.4. *It might seem confusing why we are not discussing these seemingly arbitrary operations, but not the union operation, which is a very nice set operation that we usually like to compute! But ideals are usually not closed under unions. Consider $2\mathbb{Z}$ and $3\mathbb{Z}$ as ideals of $\mathbb{Z}$, now consider $2\mathbb{Z} \cup 3\mathbb{Z}$. If this set has any hope of being an ideal, then it has to be closed under addition. Well $2 \in 2\mathbb{Z}$, and $3 \in \mathbb{Z}$, so $2 + 3 = 5 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, but $5 \notin 2\mathbb{Z}$, and $5 \notin 3\mathbb{Z}$, so $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.*

Furthermore, these operations are very useful for helping understand the relationship between algebra and certain geometric properties, such as the common set of zeroes of a collection of polynomials. It is no surprise that these operations are a favorite for algebraic geometers!

□

Problem (8)**.** *(Problem 3.51) Let I be the following subset of the ring $\mathbb{Z}[x]$ of polynomials having integer coefficients:*

$$I \;=\; \{2a(x) + xb(x) : a(x), b(x) \in \mathbb{Z}[x]\}.$$

(a) Prove that I is an ideal of $\mathbb{Z}[x]$.

(b) Prove that $I \neq \mathbb{Z}[x]$.

(c) Prove that I is not a principal ideal, i.e.*, prove that there does not exist a polynomial $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$.*

(d) Prove that I is a maximal ideal of $\mathbb{Z}[x]$.

Solution. For (a), we first show that if $\alpha, \beta \in I$, then $\alpha + \beta \in I$. We consider

$$\alpha = 2a_1(x) + xb_1(x) \qquad\qquad \beta = 2a_2(x) + xb_2(x)$$

for $a_1(x), a_2(x), b_1(x), b_2(x) \in \mathbb{Z}[x]$. Then we indeed have

$$\begin{aligned}\alpha + \beta &= 2a_1(x) + xb_1(x) + 2a_2(x) + xb_2(x)\\ &= 2a_1(x) + 2a_2(x) + xb_1(x) + xb_2(x)\\ &= 2(a_1(x) + a_2(x)) + x(b_1(x) + b_2(x)),\end{aligned}$$

where we see $a_1(x) + a_2(x) \in \mathbb{Z}[x]$ and $b_1(x) + b_2(x) \in \mathbb{Z}[x]$. Thus, we see $\alpha + \beta \in I$ by definition.
We then show that if $\alpha \in I$ and $r \in \mathbb{Z}[x]$, then $r\alpha \in I$. Define $\alpha = 2a(x) + xb(x)$ and $r = r(x)$, where $a(x), b(x), r(x) \in \mathbb{Z}[x]$. We then have

$$\begin{aligned}r\alpha &= r(x)(2a(x) + xb(x))\\ &= 2r(x)a(x) + xr(x)b(x)\end{aligned}$$

But we know $r(x)a(x), r(x)b(x) \in \mathbb{Z}[x]$. By definition, we see this means $r\alpha \in I$. This proves I is indeed an ideal of $\mathbb{Z}[x]$.

For (b), we suppose for the sake of contradiction that $I = \mathbb{Z}[x]$. This then implies we have $1 \in I$ such that we can express it as

$$1 \;=\; 2a(x) + xb(x) \quad \text{for} \quad a(x), b(x) \in \mathbb{Z}[x]$$

based on the definition of I. We then define

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \qquad b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_m.$$

By simple plugging in, we see

$$\begin{aligned} 1 &= 2(a_0 + a_1x + a_2x^2 + \cdots + a_n) + x(b_0 + b_1x + b_2x^2 + \cdots + b_m) \\ &= 2a_0 + (2a_1 + b_0)x + (2a_2 + b_1)x^2 + \cdots \end{aligned}$$

But for the equality to hold, we need $a_0 = 1/2$ and the rest of coefficients vanish for the degree to match, a contradiction.

For (c), we suppose for the sake of contradiction that there exists $c(x) \in \mathbb{Z}[x]$ such that $I = c(x)\mathbb{Z}[x]$. We see that $2 \in I$, so we must have $2 = c(x)d(x)$ for some $d(x) \in \mathbb{Z}[x]$. For this equality to hold, we need $c(x), d(x) \in \mathbb{Z}$, so we have that $c(x) \in \{\pm 1, \pm 2\}$.
Next, by looking at $1 \in I$, we must have $x = c(x)e(x)$ for some $e(x) \in \mathbb{Z}[x]$. We have previously argued that $c(x)$ is a constant, so we must have $e(x) = x$. But this then gives $c(x) = \pm 1$, so we have $I = c(x)\mathbb{Z}[x] = \mathbb{Z}[x]$. This gives a contradiction based on our result from (b) that $I \neq \mathbb{Z}[x]$.

For (d), we consider the map $\psi : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\psi(f(x)) = f(0)$ for $f(x) \in \mathbb{Z}[x]$ and $\tau : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ with $\tau(x) = x \mod 2$. We are interested in $\phi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$ defined by $\phi = \tau \circ \psi$. We see that τ and ψ are indeed both surjective so that we have ϕ is surjective. We want to show that I is the kernel of the map ϕ. We first see that $\ker(\psi) = \langle x \rangle$. Since we are modding out by 2 in the map τ, we then have $\ker(\phi) = \langle x, 2 \rangle = I$.
By First Isomorphism Theorem for Rings, we see that this then gives $\mathbb{Z}[x]/I \cong \mathbb{Z}/2\mathbb{Z}$, proving I is maximal.
□

6 Homework 7

Due Date: Tuesday, November 18
Problems:

1. (Problem 6.3) In the dihedral group $\mathcal{D}_n$, let R be a clockwise rotation by $\frac{2\pi}{n}$ radians, and let F be a flip.
   (a) Prove that the subgroup $\{e, R, R^2, \ldots, R^n\}$ is a normal subgroup of $\mathcal{D}_n$.
   (b) Let $n \geq 3$. Prove that the subgroup $\{e, F\}$ is not a normal subgroup of $\mathcal{D}_n$.
2. (Problem 6.6 abc) Let G be a group, let $H \subset G$ and $K \subset G$ be subgroups, and assume that K is a normal subgroup of G.
   (a) Prove that $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G.
   (b) Prove that $H \cap K$ is a normal subgroup of H, and that K is a normal subgroup of HK.
   (c) Prove that HK/K is isomorphic to $H/(H \cap K)$.
3. (Problem 6.13) Let G be a group, and let X be a set on which G acts.
   (a) Suppose that $\#G = 15$ and $\#X = 7$. Prove that there is some element of X that is fixed by every element of G.
   (b) What goes wrong with your proof if $\#G = 15$, and $\#X = 6$ or $\#X = 8$?
4. (Problem 6.16 ab) Let p be a prome. We proved in Corollary 6.26 that a group with p^2 elements must be abelian. Let G be a group with p^3 elements.
   (a) Mimic the proof of Corollary 6.26 to try to prove that G is abelian. Where does the proof go wrong?
   (b) Give two examples of non-abelian groups with 2^3 elements (this shows that the proof in (a) can't work).
5. (Problem 6.23) In Example 6.36 we showed that there are exactly two groups of order 10. Do a similar calculation to find all groups of order 15.

Solutions next page

Problem (1). *(Problem 6.3) In the dihedral group $\mathcal{D}_n$, let R be a clockwise rotation by $\frac{2\pi}{n}$ radians, and let F be a flip.*

(a) Prove that the subgroup $\{e, R, R^2, \ldots, R^n\}$ is a normal subgroup of $\mathcal{D}_n$.

(b) Let $n \geq 3$. Prove that the subgroup $\{e, F\}$ is not a normal subgroup of $\mathcal{D}_n$.

Solution. First note that $RF = FR^{-1}$ can be proven geometrically by looking at what the rotation and the flip do to the vertices of the $n-$gon. More formally, consider the two cases depending on whether n is odd or even.

Suppose first that F fixes some vertex (this is always the case if n is odd, and sometimes when n is even). First label the vertices $1, 2, 3, \ldots, n$ so that F fixes 2. Then the action of R and F on vertices $1, 2, 3$ is

$$R(1) = 2, \quad R(2) = 3, \quad F(1) = 3, \quad F(2) = 2, \quad F(3) = 1.$$

We use these to compute

$$RFRF(2) = RFR(2) = RF(3) = R(1) = 2,$$
$$RFRF(3) = RFR(1) = RF(2) = R(2) = 3$$

Thus $RFRF$ fixes two adjacent vertices of the $n-$gon. The rigidity of the $n-$gon implies that $RFRF$ fixes every vertex, and hence that $RFRF = e$ is the identity element of $\mathcal{D}_n$. Therefore

$$RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1},$$

where $F = F^{-1}$ follows from $F^2 = e$. In fact, this identity holds true based on the geometric interpretation of dihedral groups. If you perform the same reflection twice, you are moving vertices back to where they started, and it will always be the case that this process is the same as doing nothing.

Next suppose that F does not fix any of the vertices. This forces n to be even, and there will be two adjacent vertices that F swaps. You can think of the line of symmetry intersection the lines of the polygon instead of passing through any particular vertex. It should be clear that in order for such a line to be a line of symmetry, then n must be even. Again label the vertices as $1, 2, 3, \ldots$ so that F swaps 2 and 3. Then the action of R and F on vertices 1,2,3 is

$$R(1) = 2, \quad R(2) = 3, \quad F(1) = 4, \quad F(2) = 3, \quad F(4) = 1$$

And now use these to compute

$$RFRF(2) = RFR(3) = RF(4) = R(1) = 2,$$

$$RFRF(3) = RFR(2) = RF(3) = R(2) = 3.$$

Thus again $RFRF$ fixes adjacent vertices, so $RFRF = e$ and hence $RF = FR^{-1}$.

Now for part (a). Let $H = \{e, R, R^2, \ldots, R^{n-1} \subset \mathcal{D}_n$. For any $h \in H$ we have $h^{-1}Hh = H$, so it suffices to check the elements that are not in H. Those elements are of the form FR^i for $0 \leq i < n$. Let

$R^j \in H$. Then

$$\begin{aligned}(FR^i)^{-1}R^j(FR^i) &= R^i(FR^j)fR^i \\ &= R^{-i}(R^{-j}F)FR^i \quad \text{using} RF = FR^{-1} \\ &= R^{-i-j}F^2R^i \\ &= R^{-i-j}R^i \\ &= R^{-j} \in H\end{aligned}$$

Thus $g^{-1}Hg = H$ for all $g \in \mathcal{D}_n$, which completes the proof that H is a normal subgroup of $\mathcal{D}_n$.

For part (b), consider:

$$\begin{aligned}R^{-1}\{e, F\}R &= \{R^{-1}R, R^{-1}FR\} \\ &= \{e, (FR)R\} \quad \text{using} F = R^{-1}F, \\ &= \{e, FR^2\}.\end{aligned}$$

Thus if $\{e, F\}$ is a normal subgroup, then we must have $FR^2 = F$, which implies that $R^2 = e$ and hence that $n = 1$ or $n = 2$. As we have assumed that $n \geq 3$, we have arrived at a contradiction, which completes that proof that $\{e, F\}$ is not a normal subgroup of $\mathcal{D}_n$. □

Problem (2)**.** *(Problem 6.6 abc) Let G be a group, let $H \subset G$ and $K \subset G$ be subgroups, and assume that K is a normal subgroup of G.*

(a) Prove that $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G.

(b) Prove that $H \cap K$ is a normal subgroup of H, and that K is a normal subgroup of HK.

(c) Prove that HK/K is isomorphic to $H/(H \cap K)$.

Solution. For part (a), both H and K contain e, so $e^2 = e \in HK$, and thus the set must be nonempty. Next let $h \in H, \text{and} k \in K$, we want to check that $(hk)^{-1} \in HK$ to use the subgroup test. We have that $(hk)^{-1} = k^{-1}h^{-1}$, but since $h \in N(K)$, we also know that $hk^{-1}h^{-1} \in K$, so we see that

$$(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK.$$

Similarly, let $h_1, h_2 \in H$ and $k_1, k_2 \in K$, we can show that $h_1k_1h_2k_2 \in HK$ by deducing that

$$h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_2 \in HK.$$

In particular we have that $h_2^{-1}k_1h_2 \in K$ since $H \subset N(K)$. Thus the proof that HK is a subgroup in completed.

Now for part (b) we start by showing that $H \cap K$ is a normal subgroup of H. Let $k \in H \cap K$ and $h \in H$. Then $k \in K$, and $h \in H \subseteq N(K)$, so $h^{-1}kh \in K$. Also since $k \in H$ and $h \in H$, we have that $h^{-1}kh \in H$. Therefore $h^{-1}kh \in H \cap K$, so $H \cap K$ is a normal subgroup of H.

Remark 6.1. *We could also have proved this by first solving the homomorphism in part (c), and then deducing that the kernel of the homeomorphism is $H \cap K$, which gives us automatically that the subgroup is normal.*

Next we show that K is a normal subgroup of HK. Let $k_1 \in K$ and $hk_2 \in HK$. Then

$$(hk_2)^{-1}k_1(hk_2) = k_2^{-1}h^{-1}k_1hk_2 \in K.$$

Therefore by the same arguments as above, we have shown that K is a normal subgroup of HK.

Finally for part (c). There is a natural homomorphism $\phi : H \to HK/K$ given by $\phi(h) = hK$, where we may view $h \in H$ as an element of HK by writing h as he. We note that ϕ is surjective, since for any $hk \in HK$ we have $\phi(h) = hK = hkK$. Further, we see that $h \in \ker(\phi)$ if and only if $hK = K$, so if and only if $h \in K$. Hence $\ker(\phi) = H \cap K$, so by Theorem 6.12 in the book. □

Problem (3)**.** *(Problem 6.13))Let G be a group, and let X be a set on which G acts.*

(a) Suppose that $\#G = 15$ and $\#X = 7$. Prove that there is some element of X that is fixed by every element of G.

(b) What goes wrong with your proof if $\#G = 15$, and $\#X = 6$ or $\#X = 8$?

Solution. Since $\#G = 15$, Cauchy's theorem tells us that the only possible order for a subgroup of G is either $1, 3, 5$, or 15, so for every i, we have

$$\#G_{x_i} = \frac{\#G}{\#G_{x_i}} = 1, 3, 5, \text{ or } 15.$$

Hence every term in the Orbit-Stabilizer Counting Theorem is equal to $1, 3, 5$, or 15, so

$$7 = \#X = (\text{some } 1'\text{s}) + (\text{some } 3'\text{s}) + (\text{some } 5'\text{s}) + (\text{some } 15'\text{s}).$$

But the only ways to write 7 are

$$\begin{aligned} 7 &= 1+1+1+1+1+1+1, \\ 7 &= 1+1+1+1+3, \\ 7 &= 1+3+3, \\ 7 &= 1+1+5. \end{aligned}$$

Hence there is at least one element $x \in X$ with $\#Gx = 1$, so $G_x = 15$ so x is fixed by every element of G.

For part (b), notice that for $\#X = 6 = 3 + 3$, then applying the Orbit-Stabilizer Counting Theorem might yield two orbits, each consisting of 3 elements. Similarly if $\#X = 8 = 3 + 5$, then there must be two orbits, one with 3 elements, and one with 5 elements. □

Problem (4)**.** *(Problem 6.16 ab) Let p be a prome. We proved in Corollary 6.26 that a group with p^2 elements must be abelian. Let G be a group with p^3 elements.*

(a) Mimic the proof of Corollary 6.26 to try to prove that G is abelian. Where does the proof go wrong?

(b) Give two examples of non-abelian groups with 2^3 elements (this shows that the proof in (a) can't work).

Solution. For part (a). Changing p^2 to p^3 in the first line of the proof gives:

Lagrange tells us that the order of the center $Z(G)$ divides $\#G = p^3$, so $\#Z(G) = 1, p, p^2$, or p^3. We know from the theorem that $Z(G)$ is non-trivial, since the theorem applies to groups of any prime order, so $\#Z(G) \neq 1$.

We want to rule out $\#Z(G) = p$ and $\#Z(G) = p^2$. The proof of the corollary actually works out for the latter.

Thus suppose that $\#Z(G) = p^2$. This means that we can find some $g \in G$ with $g \notin Z(G)$. The centralizer of g satisfies

$$Z_G(g) \supseteq Z(G) \cup \{g\},$$

since g commutes with every element of $Z(G)$ by definition of $Z(G)$, and certainly g commutes with itself. Since $g \notin Z(G)$, we see that

$$\#Z_G(g) \geq \#Z(G) + \#\{g\} = p^2 + 1.$$

But $Z_G(g)$ is a subgroup of G, so its order divides $\#G$ by Lagrange's theorem. The only number larger than $p^2 + 1$ that divides p^3 is p^3 itself, so

$$Z_G(g) = p^3 = \#G.$$

It follows that $Z_G(g) = G$, which means that every element of G commutes with g, which means that $g \in Z(G)$. This contradicts the assumption that $g \notin Z(G)$ made above. So we have proven that $\#Z(G) \neq p^2$.

We would now like to use the same sort of argument to prove that $\#Z(G) \neq p$, but the proof doesn't work. Here's what happens if we try. Suppose that $\#Z(G) = p$. As before, we look at some $g \in G$ with $g \notin Z(G)$, and as before the centralizer of g satisfies:

$$Z_G(g) \supseteq Z(G) \cup \{g\}.$$

Since $g \notin Z(G)$, we see that

$$\#Z_G(g) \geq \#Z(G) + \#\{g\} = p + 1.$$

But since $Z_G(g)$ is a subgroup of G, so its order divides $\#G$ by Lagrange's theorem. Now there are two numbers larger than $p + 1$ that divide p^3, namely p^2 and p^3. So we can only say that either $\#Z_G(g) = p^2$ or $\#Z_G(g) = p^3$. Certainly the same logic as above prevents $\#Z_G(g) = p^3$. Now then it follows that one of the following claims must be true

1. G is abelian, and as such it is not a problem that $Z(G) = p^3$. In fact this just demonstrates that out proof breaks down at the assumption of the existence of an element in G that is not in $Z(G)$.

2. $\#Z(G) = p$ and $\#Z_G(g) = p^2$ for every $g \notin Z(G)$.

At this point we are stuck because there may well exist non-abelian groups of order p^3 that satisfy (2).

Now for part (b). The dihedral group $\mathcal{D}_4$ and the quaternion group $\mathcal{Q}$ are non-abelian groups of order 8. They are not isomorphic, since, for example $\mathcal{D}_4$ has only 2 elements of order 4, while $\mathcal{Q}$ has 6 such elements. However, they both have centralizer of order 2, and the centralizer of every non-central element has order 4, which gives us an example of two non-abelian groups that satisfy property (2) from the proof above.

Remark 6.2. *In particular this provides excellent reason as to why the extension of the theorem to p^3 is so difficult, because it is not true! Occasionally theorems that seem like they should be true have to sneakily assume commutativity in order to hold. For a particularly nasty example, try to prove for an arbitrary ring, R, $R^n \cong R^m$ if and only if $n = m$!*

□

Problem (5)**.** *(Problem 6.23) In Example 6.36 we showed that there are exactly two groups of order 10. Do a similar calculation to find all groups of order 15.*

Solution. Let k_5 be the number of 5-Sylow subgroups. Then $k_5 \mid 15$ and $k_5 \equiv 1 (\text{mod } 5)$, so $k_5 = 1$. Similarly, letting k_3 be the number of 3-Sylow subgroups, we have $k_3 = 15\text{m}$ and $k_3 \equiv 1 (\text{mod } 3)$, so $k_3 = 1$. Hence G has a unique 3 and 5-Sylow subgroups H_2 and H_5, which are thus also normal. As argument similar to that in the example shows that $H_3 \cap H_5 = \{e\}$, and indeed, in general for subgroups A and B, if $\gcd(\#A, \#B) = 1$, then $A \cap B = \{e\}$. It follows from an earlier exercise that the map $\phi : H_3 \times H_5 \to G$, where $\phi(a, b) = ab$ is an injective mapping, and since the domain and range each have 15 elements, then it is a bijective mapping set-wise. Being very specific about how we write H_3 and H_5, we see:

$$H_3 = \{e, a, a^2\} \text{ and } H_5 = \{e, b, b^2, b^3, b^4\}.$$

The bijectivity of ϕ means every element of G has the form $a^i b^j$ with $i \in \{0, 1, 2\}$, $j \in \{0, 1, 2, 3, 4\}$. Consider the element aba^{-1}. It has order 5, so it is in H_5, since there is only one 5-Sylow subgroup. So $aba^{-1} = b^n$ for some $0 \leq n \leq 4$. We use this to compute

$$\begin{aligned} b = a^{-1}b^n a = (a^{-1}ba)^n = (a^{-2}aba^{-1}a^2)^n \\ = (a^{-2}b^n a^2) = (ab^n a^{-1})^n = (aba^{-1})^{n^2} = b^{n^2} \end{aligned}$$

Since b has order 5, it follows that $n^3 \equiv 1 (\text{mod } 5)$.

Now checking $n = 0, 1, 2, 3, 4$, this implies that $n = 1$. Hence $aba^{-1} = b$ i.3., $ab = ba$. This prove that every element of H_3 commutes with every element of H_5, which in turn implies that ϕ is a group homomorphism, which proves that every group of order 15 is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, which is in turn isomorphic to $\mathbb{Z}/15\mathbb{Z}$. □