

Solution to Algebra : Chapter 0 by Paolo Aluffi

macyayaya¹

Last updated at February 23, 2020
v0.4.2

¹<https://github.com/macyayaya/>

Copyright (C) 2020 macyayaya @ <https://github.com/macyayaya/>.
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with the Invariant Sections being Prologue. A copy of the license is included in the section entitled "GNU Free Documentatin License".

Prologue

Over a few months I want to improve my skills in solving algebra problems. I tried to find a textbook that can serves me good and is good enough to use in self-study.

Eventually, this is what I felt the most "comfortable" book in my opinion. It doesn't contain that much unlike Dummit & Foote, but the writing style, the explanation, and the exercises really served me well.

So here is the solution to Algebra : Chapter 0. There are a few important points to note here:

- The solution is *only* hosted on my GitHub page <https://github.com/macyayaya/algebra-chapter-0-solutions>. If you find this document outside this page, you might have an outdated version of the solution which might have errors, so please be aware.
- I will update the solution irregularly.
- I'll try to write this beginner-friendly (as I am also a beginner), so the answer might be way too detailed/verbose. Sorry if you find this annoying.
- If you found an error in the solutions, typos, bad grammar or want to give an advise on LaTeX formatting, etc., don't hesitate to open an issue or a pull request on my repo.
- The questions I picked is completely random, so if you want to see some solution of a certain problem (but please not all of them), you can also open an issue to notify me.
- However, I currently do *not* accept any PRs to new solutions; this is more than my note on self-study rather than a complete solution set.

Thanks.

macyayaya @ <https://github.com/macyayaya/>
Department of Mathematics, National Taiwan University
February 16, 2020

Contents

Prologue	ii
I Preliminaries: Set theory and categories	1
I.1	1
I.2	1
I.3	2
I.4	4
I.5	4
II Groups, first encounter	7
II.1	7
II.2	8
II.3	8
II.4	9
II.5	11
II.6	11
II.7	13
II.8	14
II.9	16
III Rings and modules	18
III.1	18
III.2	19
III.3	21
III.4	23
III.5	26
III.6	28
III.7	32
IV Groups, second encounter	34
IV.1	34
IV.2	35
	38

Chapter I

Preliminaries: Set theory and categories

Throughout this solution manual, we will use the same notation (and convention) as in the book, with probably a little to none changes.

For your convenience, it is recommended to search your question via whatever your browser provides (e.g. F3). The format of questions are *Chapter*(in roman).*Section*.*Question*.

In the following, categories are denoted using the **Sans-serif** font, e.g. **Set**.

I.1

Problem I.1.1. Locate a discussion of Russel's paradox, and understand it.

Problem I.1.2. Prove that if \sim is an equivalence relation on a set S , then the corresponding family \mathcal{P}_\sim defined in §1.5 is indeed a partition of S .

Proof. The union of such class must contain S by definition, as at worse the elements can be in the equivalence class formed by themselves. It suffices to check disjointness: If $a \in [x], a \in [y]$ but $x \not\sim y$, then transitivity implies $x \sim a, a \sim y \Rightarrow x \sim y$, a contradiction. ■

I.2

Problem I.2.1. How many different bijection are there between a set S with n elements and itself?

Solution. The first number has n choices; to make the map a bijection, the next number has only $(n - 1)$ choices remaining. By continuing choosing, we have $n!$ different bijections. ■

Problem I.2.5. Formulate a notion of *epimorphism*, in the style of the notion of *monomorphism*, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.

Solution. Epimorphism are *right-cancelable*; that is,

A function $f : A \rightarrow B$ is a epimorphism if for all sets Z and all functions $\beta, \beta' : Z \rightarrow A$,

$$\beta \circ f = \beta' \circ f \implies \beta = \beta'.$$

We shall prove the following:

Proposition. *A function is surjective if and only if it is an epimorphism.*

Proof.

(\Rightarrow) Let f be surjective. By Proposition I.2.1, a surjective function has a right-inverse, which we

call it g . Then if $\beta, \beta' : B \rightarrow Z$ are arbitrary function such that $\beta \circ f = \beta' \circ f$, then by composition with g we obtain

$$(\beta \circ f) \circ g = (\beta' \circ f) \circ g \Rightarrow \beta \circ (f \circ g) = \beta' \circ (f \circ g) \Rightarrow \beta \circ id_A = \beta' \circ id_A \Rightarrow \beta = \beta'$$

as desired.

(\Leftarrow) Let f be an epimorphism. We need to consider some special $\beta : B \rightarrow Z$ so we can prove the assertion. We done this by "labeling": define

$$\beta(b) = \begin{cases} 1, & b \in \text{im } f \\ 0, & b \notin \text{im } f \end{cases}, \quad \beta'(b) = 1$$

Then since

$$\beta \circ f = \beta' \circ f \Rightarrow \beta = \beta'$$

this implies that beta receives *only* values in $\text{im } f$, so $\text{im } f \supseteq B$. Since we have $\text{im } f \subseteq B$ clearly for any function f , we conclude that $\text{im } f = B$, which is the definition of surjectivity. ■

I.3

Problem I.3.1. Let \mathbf{C} be a category. Consider a structure \mathbf{C}^{op} with

- $\text{Obj}(\mathbf{C}^{op}) = \text{Obj}(\mathbf{C})$;
- for A, B objects of \mathbf{C}^{op} , $\text{Hom}_{\mathbf{C}^{op}}(A, B) := \text{Hom}_{\mathbf{C}}(B, A)$.

Show how to make this into a category.

Solution. For $f \in \text{Hom}_{\mathbf{C}^{op}}(A, B), g \in \text{Hom}_{\mathbf{C}^{op}}(B, C)$, define the composite of morphisms by

$$g \circ f := fg$$

where fg is defined in the sense of the category \mathbf{C} . Now we check the definition of category:

- 1_A exists as $\text{Hom}_{\mathbf{C}^{op}}(A, A) := \text{Hom}_{\mathbf{C}}(A, A) \ni 1_A$;
- The composition works as intended: the map on the right is a morphism from C to A ;
- The composite law is checked as

$$(h \circ g) \circ f = gh \circ f = f(gh) = (fg)h = h \circ fg = h \circ (g \circ f);$$

- Identity morphism work as intended:

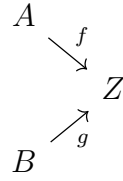
$$1_A \circ f = f1_A = f, \quad f \circ 1_A = 1_A f = f.$$

■

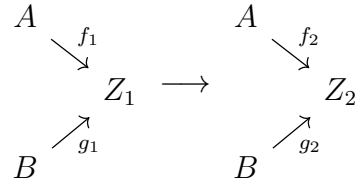
Problem I.3.11. Draw the relevant diagrams and define composition and identities for the category $\mathbf{C}^{A,B}$ mentioned in Example 3.9. Do the same for the category $\mathbf{C}^{\alpha,\beta}$ mentioned in Example 3.10.

Solution. By reversing the arrow of $\mathbf{C}_{A,B}$, we obtain:

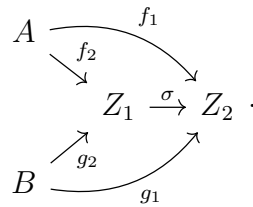
- Objects of this category are diagrams



- morphisms are

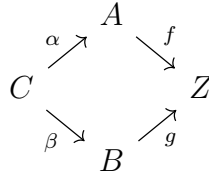


which are commutative diagrams

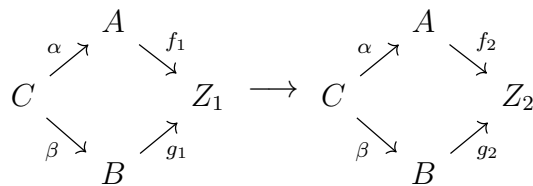


For the case $\mathbf{C}^{\alpha, \beta}$:

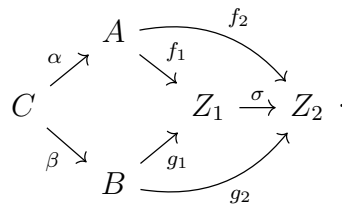
- Objects are diagrams



- morphisms are



which are commutative diagrams



composition and identity are defined analogously as in Example 3.5. ■

I.4

Problem I.4.3. Let A, B be objects of a category \mathbf{C} , and let $f \in \text{Hom}_{\mathbf{C}}(A, B)$ be a morphism.

- Prove that if f has a right-inverse, then f is an epimorphism.
- Show that the converse does not hold, by giving an explicit example of a category and an epimorphism without a right-inverse.

Proof. Let g be the right inverse of f , i.e. $fg = 1$. Then for any morphism $h, h' \in \text{Hom}_{\mathbf{C}}(B, Z)$,

$$h \circ f = h' \circ f \Rightarrow h \circ f \circ g = h' \circ f \circ g \Rightarrow h \circ 1 = h' \circ 1 \Rightarrow h = h'$$

showing that f is an epimorphism. For a counterexample in which the converse does not hold, consider $\mathbf{C} = \mathbb{Z}$, objects are integers, and morphisms are the relation \leq (c.f. p.p.27). Then

$$f : 1 \rightarrow 2$$

is an epimorphism, but there are no right inverse for f , since there are no morphisms in $\text{Hom}_{\mathbf{C}}(2, 1)$. ■

I.5

Problem I.5.1. Prove that a final object in a category \mathbf{C} is initial in the opposite category \mathbf{C}^{op} (I.3.1).

Proof. Let F be a final object in \mathbf{C} , which means that the set $\text{Hom}_{\mathbf{C}}(A, F)$ is a singleton for all $A \in \text{Obj}(\mathbf{C})$. Since

$$\text{Hom}_{\mathbf{C}}(A, F) = \text{Hom}_{\mathbf{C}^{op}}(F, A)$$

we have that F is initial in \mathbf{C}^{op} . ■

Problem I.5.12. Define the notions of *fibered products* and *fibered coproducts*, as terminal objects of the categories $\mathbf{C}_{\alpha, \beta}, \mathbf{C}^{\alpha, \beta}$ considered in Example 3.10 (cf. also I.3.11), by stating carefully the corresponding universal properties.

As it happens, **Set** has both fibered products and fibered coproducts. Define these objects 'concretely', in terms of naive set theory.

Solution. Fibered product is *final* in $\mathbf{C}_{\alpha, \beta}$; that is, there are only one morphism in

$$\text{Hom} \left(\begin{array}{ccc} & A & \\ f_a \nearrow & & \searrow \alpha \\ Z & & C \\ f_b \searrow & & \nearrow \beta \\ & B & \end{array} , \begin{array}{ccc} & A & \\ i_a \nearrow & & \searrow \alpha \\ F & & C \\ i_b \searrow & & \nearrow \beta \\ & B & \end{array} \right)$$

for any choice of the triple (Z, f_a, f_b) . Expand this to a diagram leads to the following universal property:

The triple $(F, i_a : F \rightarrow A, i_b : F \rightarrow B)$ is universal in the sense that for every triple $(Z, f_a : Z \rightarrow A, f_b : Z \rightarrow B)$, there exists a unique morphism $\varphi : Z \rightarrow F$ such that the diagram

$$\begin{array}{ccccc} Z & & \xrightarrow{f_a} & A & \\ & \searrow \exists! \varphi & & \downarrow i_a & \\ & & F & \xrightarrow{i_a} & A \\ & & \downarrow i_b & & \downarrow \alpha \\ & & B & \xrightarrow{\beta} & C \\ & \swarrow f_b & & & \end{array}$$

commutes. Fibered product are also called *pullback*.

Fibered coproduct is *initial* in $\mathbf{C}^{\alpha, \beta}$. Following the same argument as above, we have the following universal property:

The triple $(I, i_A : A \rightarrow I, i_B : B \rightarrow I)$ is universal in the sense that for every triple $(Z, f_A : A \rightarrow Z, f_B : B \rightarrow Z)$, there exists a unique morphism $\varphi : I \rightarrow Z$ such that the diagram

$$\begin{array}{ccc}
 C & \xrightarrow{\alpha} & A \\
 \beta \downarrow & & \downarrow i_A \\
 B & \xrightarrow{i_B} & I
 \end{array}
 \begin{array}{c}
 \searrow f_A \\
 \downarrow \exists! \varphi \\
 \searrow f_B \\
 Z
 \end{array}$$

commutes. Fibered coproduct are also called *pushout*.

Set has fibered products: Let us define

$$A \times_C B := I = \{(a, b) : a \in A, b \in B, \alpha(a) = \beta(b)\}$$

with projections i_a, i_b . We check that this satisfy the universal property: define

$$\varphi(z) := (f_a(z), f_b(z))$$

we check:

- $i_b \varphi = f_b$ (resp. $i_a \varphi = f_a$):

$$i_b \varphi(z) = i_b(f_a(z), f_b(z)) = f_b(z)$$

- $\alpha i_a = \beta i_b$:

$$\alpha i_a(a, b) = \alpha(a) \stackrel{!}{=} \beta(b) = \beta i_b(a, b).$$

note that $!$ is true since I gurantees the existence of b .

Set also has fibered coproducts, but it's more complicated. We first define an equivalence relation: define

$$R = \{(\alpha(x), 0) \sim (\beta(x), 1) : x \in C\}$$

This gives an equivalence relation on $A \amalg B$, which gives a new structure $I = (A \amalg B) / \sim$. Let $i_A(a) = (a, 0), i_B(b) = (b, 1)$, then it is direct that $i_B \beta = i_A \alpha$. Now we define

$$\varphi[i = (x, c)] = \begin{cases} f_A(x) & \text{if } c = 0 \\ f_B(x) & \text{if } c = 1 \end{cases}$$

We need to check that it is well-defined, then it is direct that $\varphi \beta = f_B$ (resp. $\varphi \alpha = f_A$), proving the universal property. There are two cases to consider:

- Case $[(a, 0)] = [(a', 0)]$ (resp. $[(b, 1)] = [(b', 1)]$): If there are relations

$$a = \alpha(x) \sim \beta(x) = \beta(x') \sim \alpha(x') = a'$$

then they evaluated to the same value since

$$\varphi[(a, 0)] = \varphi i_A(a) = \varphi i_A(\alpha(x)) = \varphi i_B(\beta(x)) = \varphi i_B(\beta(x')) = \varphi i_A(\alpha(x')) = \varphi i_A(a') = \varphi[(a', 0)]$$

- Case $[(a, 0)] = [(b, 1)]$: If there are relations

$$a = \alpha(x) \sim \beta(x) = b$$

then

$$\varphi[(a, 0)] = \varphi i_A(a) = \varphi i_A(\alpha(x)) = \varphi i_B(\beta(x)) = \varphi i_B(b) = \varphi[(b, 1)]$$

as desired.

By the above analysis, as all elements in the same equivalence class connects to the other by some chain

$$a = \alpha(x_1) \sim \beta(x_1) = \beta(x_2) \sim \alpha(x_2) = \alpha(x_3) \cdots = b,$$

and since every \sim preserves the result, φ is well-defined. ■

Chapter II

Groups, first encounter

Unless otherwise specified, in the following G denotes a group, e denotes the identity of G . Some description and hints are omitted for simplicity.

II.1

Problem II.1.8. Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$.

Proof. For all elements that is not of order 2, they have an inverse that is not itself, so they canceled out in the product $\prod_{g \in G} g$, leaving only elements that is of order 2, i.e. f . ■

Problem II.1.10. If the order of g is odd, what can you say about the order of g^2 ?

Solution. The order of g^2 is $|g|$ since the only number that divides $|g|$ and in $\{2, 4, \dots, 2|g|\}$ is $2|g|$ if $|g|$ is odd. ■

Problem II.1.11. Prove that for all g, h in a group G , $|gh| = |hg|$.

Proof. Simply observe that $e = (gh)^{|gh|} = g(hg)^{(|gh|-1)}h$, therefore

$$g^{-1}h^{-1} = (hg)^{-1} = (hg)^{|gh|-1}$$

hence $(hg)^{|gh|} = e$. The other case $((gh)^{|hg|} = e)$ is the same. ■

Problem II.1.13. Give an example showing that $|gh| \neq \text{lcm}(|g|, |h|)$ even if g and h commute.

Solution. In C_4 , $|1 + 3| = |0| = 1$ but $\text{lcm}(|1|, |3|) = 4$. Clearly C_4 is abelian. ■

Problem II.1.14. As a counterpoint of II.1.13, prove that if g and h commute and $\text{gcd}(|g|, |h|) = 1$, then $|gh| = |g||h|$.

Proof. One has $|gh|$ divides $\text{lcm}(|g|, |h|) = |g||h|$ by Proposition II.1.14, so it suffices to prove that $|g||h|$ divides $|gh|$. Let $N = |gh|$. By noting that $(gh)^N = g^N h^N$ since g and h commutes, we have

$$(gh)^{N|h|} = e^{|h|} = g^{N|h|} h^{N|h|} = g^{N|h|}$$

so $|g|$ divides $N|h|$, which implies $|g|$ divides N since $\text{gcd}(|g|, |h|) = 1$. Similarly $|h|$ divides N , therefore $|g||h|$ divides $N = |gh|$, as desired. ■

Problem II.1.15. Let G be a commutative group, and let $g \in G$ be an element of maximal finite order. Prove that if h has finite order in G , then $|h|$ divides $|g|$.

Proof. Suppose that $|h|$ does not divide $|g|$, then we can assume that $|g| = p^m r$, $|h| = p^n s$, where p is a prime, r, s relatively prime to p and $m < n$. Since $|h|$ does not divide $|g|$, $\text{gcd}(h, g) = 1$. Then by II.1.14 we can calculate the order of $g^{p^m} h^s$, which is $p^n r$. But this element has order bigger than g , which contradicts to the maximality of g . Hence $|h|$ must divide $|g|$. ■

II.2

Problem II.2.10. Prove that $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

Proof. Trivial. ■

Problem II.2.14. Show that the multiplication in $\mathbb{Z}/n\mathbb{Z}$ is a well-defined action.

Proof. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a = a' + kn$, $b = b' + ln$ for $k, l \in \mathbb{Z}$, therefore

$$(ab) - (a'b') = (a' + kn)(b' + ln) - a'b' = a'ln + b'kn + kln^2 \equiv 0 \pmod{n}$$

as desired. ■

Problem II.2.16. Find the last digit of $1238237^{18238456}$.

Solution. $1238237^{18238456} \equiv 7^{18238456} = 49^{9119228} = 2401^{4559614} \equiv 1^{4559614} = 1 \pmod{10}$. ■

Problem II.2.17. Show that if $m \equiv m' \pmod{n}$, then $\gcd(m, n) = 1$ if and only if $\gcd(m', n) = 1$.

Proof. We can write $m = nk + m'$ for $n \in \mathbb{Z}$ and use Euclidean Algorithm to conclude. ■

II.3

Problem II.3.1. Let $\varphi : G \rightarrow H$ be a morphism in a category \mathcal{C} with products. Explain why there is a unique morphism $(\varphi \times \varphi) : G \times G \rightarrow H \times H$ compatible in the evident way with the natural projections.

Solution. The compatibility of $(\varphi \times \varphi)$ comes from the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \uparrow \pi_2 & & \uparrow \rho_2 \\ G \times G & \xrightarrow{\exists!(\varphi \times \varphi)} & H \times H \\ \downarrow \pi_1 & & \downarrow \rho_1 \\ G & \xrightarrow{\varphi} & H \end{array}$$

which is easy to check. The uniqueness follows from the universal property of products that there is a unique homomorphism such that the diagram

$$\begin{array}{ccc} & & H \\ & \nearrow & \\ G \times G & \xrightarrow{\exists!(\varphi \times \varphi)} & H \times H \\ & \searrow & \\ & & H \end{array}$$

commutes. ■

Problem II.3.3. Show that if G, H are abelian groups, then $G \times H$ satisfies the universal property for coproducts in **Ab**.

Proof. Let A be an arbitrary abelian group, f_G, f_H be homomorphisms, i_G, i_H be inclusions. We are required to prove the commutativity of the diagram

$$\begin{array}{ccccc}
 G & & & & \\
 & \searrow i_G & & \nearrow f_G & \\
 & & G \times H & \xrightarrow{\exists! \varphi} & A \\
 & \nearrow i_H & & \searrow f_H & \\
 H & & & &
 \end{array}$$

To check the universal property, define $\varphi(g, h) := f_G(g)f_H(h)$. It is direct that the diagram commutes. Finally, φ is a homomorphism since for $g_1, g_2 \in G, h_1, h_2 \in H$,

$$\begin{aligned}
 \varphi((g_1, h_1)(g_2, h_2)) &= \varphi(g_1g_2, h_1h_2) = f_G(g_1g_2)f_H(h_1h_2) = f_G(g_1)f_G(g_2)f_H(h_1)f_H(h_2) \\
 &\stackrel{\text{abelian}}{=} f_G(g_1)f_H(h_1)f_G(g_2)f_H(h_2) = \varphi(g_1, h_1)\varphi(g_2, h_2)
 \end{aligned}$$

as desired. ■

Problem II.3.6. Consider the product $C_2 \times C_3$, which is a coproduct in **Ab**. Show that it is *not* a coproduct of C_2 and C_3 in **Grp**.

Proof. If $C_2 \times C_3$ is a coproduct, then take $A = S_3$. Although there are injective homomorphisms

$$\begin{aligned}
 \varphi_1 : C_2 &\rightarrow S_3 \text{ by } \varphi_1(1) = (12) \text{ or other two cycle} \\
 \varphi_2 : C_3 &\rightarrow S_3 \text{ by } \varphi_2(1) = (123) \text{ or other three cycle}
 \end{aligned}$$

but there are no homomorphisms $\varphi : C_2 \times C_3 \rightarrow S_3$ that satisfies the universal property of coproducts: Observe that any choice of cycles in φ_1 and φ_2 will exhaust all possible element of S_3 , hence forces φ to be an isomorphism. But the element $\varphi(1, 1)$ must be either a 2(or 3)-cycle (i.e. $\varphi^2(1, 1)$ (or $\varphi^3(1, 1)$) is zero), and neither $(1, 1)^2$ nor $(1, 1)^3$ are $(0, 0)$, and φ will map a non-identity element to the identity, a contradiction (since φ is an isomorphism and must map $(0, 0)$ to the trivial cycle). ■

II.4

Problem II.4.3. Prove that a group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if and only if it contains an element of order n .

Proof. Let G be such group.

(\Rightarrow) Trivial.

(\Leftarrow) Let g be an element of order n . Then consider a homomorphism $\varphi : G \rightarrow \mathbb{Z}/n\mathbb{Z}$ with $\varphi(g) = \bar{1}$. It is a direct check that this is an isomorphism. ■

Problem II.4.8. Let $g \in G$. Prove that the function $\gamma_g : G \rightarrow G$ defined by $\gamma_g(a) = gag^{-1}$ is an automorphism of G . Prove that the function $G \rightarrow \text{Aut}(G)$ defined by $g \rightarrow \gamma_g$ is a homomorphism, and show that this homomorphism is trivial if and only if G is abelian.

Proof. γ_g is injective since if $gag^{-1} = gbg^{-1}$ then $a = b$; it is surjective since for $k \in G$ we can find $g^{-1}kg$ so that $\gamma_g(g^{-1}kg) = k$; it is a homomorphism since

$$\gamma_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b).$$

If G is abelian then the automorphism is simply $\gamma_g(a) = a$; conversely if $gag^{-1} = a$ then $ga = ag$ for all $a, g \in G$, hence abelian. ■

Problem II.4.9. Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$.

Proof.

$$\varphi : C_{mn} \rightarrow C_m \times C_n, \varphi(a) = (a \bmod m, a \bmod n)$$

is a homomorphism and a bijection. ■

Problem II.4.11. Assuming the fact that the equation $x^d = 1$ can have at most d solutions in $\mathbb{Z}/p\mathbb{Z}$ for a prime p , prove that $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Proof. Let g be an element of maximal order, and by II.1.15, all elements have degree that divides $|g|$, i.e. $|h|^{[g]} = 1$ for all $h \in G$. Using the fact, we have $|G| \leq |d|$, since only at most $|g|$ elements can be the solution to $h^{[g]} = 1$. Clearly we also have $|G| \geq |d|$, so $|G| = |d|$. Thus the proof is complete by II.4.3. ■

Problem II.4.13. Prove that $\text{Aut}_{\text{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$.

Proof. To make an automorphism φ , φ must fix $(0, 0)$, leaving 6 possible permutations for elements $(0, 1), (1, 0), (1, 1)$. It suffices to check that all permutations of these elements are homomorphisms (hence isomorphisms). ■

Problem II.4.14. Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r \leq n$ that are *relatively prime* to n (cf. II.6.14).

Proof. We shall first show that every endomorphism of cyclic group C is of form $\varphi_n(x) = x^n$ for some n . Indeed, if σ is an endomorphism that $\sigma(x) = x^a = \varphi_a(x)$, then for every $x^b \in C$ we have

$$\sigma(x^b) = \sigma(x)^b = (x^a)^b = (x^b)^a = \varphi(x^b)$$

so every endomorphism is of form $\varphi_n : x \mapsto x^n$ for some n . Now to make this into an automorphism, if k is not relatively prime to n , say $\gcd(n, k) = r > 1$, then for a generator $x \in C_n$, we have

$$\varphi_k(x^{n/r}) = x^{n/r \cdot k} = x^{n \cdot k/r} = (x^n)^{k/r} = e^{k/r} = e$$

and since n/r is not n , φ_k maps a non-identity element to e , in which it is already mapped by $e \in C_n$, so φ_k fails to be a bijection. Therefore the order of $\text{Aut}(C_n)$ is the number of positive integers that is relatively prime to n . ■

Problem II.4.16. Prove the *Wilson's theorem*: for $p \in \mathbb{N}_{>1}$, p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}$$

Proof. (\Rightarrow) Assuming that the result of II.1.8 and II.4.11 is true, consider $G = (\mathbb{Z}/n\mathbb{Z})^*$. It is cyclic, and has exactly one element of order 2 since for $0 \leq k \leq p-2$,

$$(p-1-k)^2 \equiv 1 + 2k + k^2 \equiv 1 \pmod{p} \iff k(k+2) \equiv 0 \pmod{p}$$

and such solution can only be $k = 0$ or $p-2$ since p is a prime, which correspond to $p-1$ and 1 (identity). Therefore by II.1.8

$$\prod_{g \in G} g = (p-1)! \equiv (p-1) \equiv -1 \pmod{p}$$

as desired.

(\Leftarrow) If p is not a prime, then there exists $1 < k < p$ such that $k|p$. Since $k < p$ we have $k|(p-1)!$, i.e.

$$(p-1)! \equiv rk \pmod{p} \text{ for some } r \in \mathbb{Z}$$

and clearly no choice of r will make $rk \equiv -1 \pmod{p}$ by the fact that $k|p$. Therefore p must be a prime. ■

II.5

Problem II.5.3. Use the universal property of free groups to prove that the map $j : A \rightarrow F(A)$ is injective.

Proof. If there is $a, b \in A$ such that $j(a) = j(b)$ but $a \neq b$, then let f be a set function such that $f(a) \neq f(b)$; in particular, let $G = \mathbb{Z}$ and let $f(a) = 1, f(b) = 2$. Then there are no homomorphisms that will make the diagram commute, therefore j must be injective. ■

Problem II.5.6. Prove that the group $F(\{x, y\})$ is a coproduct $\mathbb{Z} * \mathbb{Z}$ of \mathbb{Z} by itself in the category Grp.

Proof. We are given the universal property of free group: for $j : \{x, y\} \rightarrow F(\{x, y\})$, $\exists G, f$ such that the diagram

$$\begin{array}{ccc} F(\{x, y\}) & \xrightarrow{\exists! \varphi} & G \\ j \uparrow & \nearrow f & \\ \{x, y\} & & \end{array}$$

commutes. To check that it is a coproduct, consider the coproduct diagram composed with above. Let $i(0) = x, j$ be the inclusion, then we have the following diagram:

$$\begin{array}{ccccc} & & \mathbb{Z} & \xrightarrow{f} & \\ & \nearrow \gamma & & \searrow i & \\ \{x, y\} & \xrightarrow{j} & F(\{x, y\}) & \xrightarrow{\exists! \varphi} & G \\ & \searrow \gamma & & \nearrow i & \\ & & \mathbb{Z} & \xrightarrow{g} & \end{array}$$

g

Note that the arrows j, g, φ comes from the free group diagram. From this, we have $f \circ \gamma = \varphi \circ j$. To check the coproduct diagram commutes, it suffices to check $f = \varphi \circ i$ (the case $g = \varphi \circ i$ is identical). To do this, define $\gamma(x) = 0, \gamma(y) = 1$. Then

$$f \circ \gamma(x) = f(0) = \varphi(x) = \varphi \circ j(x), \quad f \circ \gamma(y) = f(1) = \varphi(y) = \varphi \circ j(y)$$

Since $f(1) = \varphi \circ i(1) = \varphi(y)$, the homomorphisms agree on the generator, hence are the same. ■

II.6

Problem II.6.5. Let G be a commutative group, and let $n > 0$ be an integer. Prove that $\{g^n : g \in G\}$ is a subgroup of G . Prove that this is not necessarily the case if G is not commutative.

Proof. For any two elements a, b in the set, they can be represented as g^n and h^n respectively. Now

$$ab^{-1} = g^n h^{-n} = (gh^{-1})^n$$

which shows that ab^{-1} is also in the set, proving the set is a subgroup. A counterexample would be D_6 , the dihedral group with 6 elements, with the choice $n = 3$. Let s denote the reflection, r denotes the rotation, we then have

$$\{g^3 : g \in D_3\} = \{1, r^3, r^{2 \cdot 3}, s^3, (sr)^3, (sr^2)^3\} = \{1, 1, 1, s, sr, sr^2\}$$

this set is not a subgroup, as $s^{-1}sr = r$ is not an element of this set. ■

Problem II.6.7. Show that inner automorphisms (the collection of γ_g in II.4.8) form a subgroup $\text{Inn}(G)$ of $\text{Aut}(G)$, and show that $\text{Inn}(G)$ is cyclic if and only if $\text{Inn}(G)$ is trivial if and only if G is abelian. Deduce that if $\text{Aut}(G)$ is cyclic, then G is abelian.

Proof. $\text{Inn}(G)$ is a subgroup since

$$\gamma_g \circ \gamma_{h^{-1}} = gh^{-1}ahg^{-1} = (gh^{-1})a(gh^{-1})^{-1} \in \text{Inn}(G).$$

If $\text{Inn}(G)$ is cyclic, then let $\gamma_g(a) = gag^{-1}$ be a generator of order n . Then for any $b \in G$, we have $\gamma_b(x) = \gamma_g^n(x)$, for some integer n . Then by plug in b into the homomorphism, we have $gbg^{-1} = b^nbb^{-n}$. This gives $gb = bg \ \forall b \in G$, so γ_g is in fact trivial. Since the generator is trivial, we conclude that $\text{Inn}(G)$ is trivial. If $\text{Inn}(G)$ is trivial, then the function given in II.4.8 can only be the trivial map, so G is abelian by II.4.8. Finally, if G is abelian, then all inner automorphisms are trivial, and clearly trivial group is cyclic.

The last statement follows from Proposition II.6.11 that every subgroup of cyclic group is cyclic. ■

Problem II.6.9. Prove that an *abelian* group G is finitely generated if and only if there is a surjective homomorphism

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}} \twoheadrightarrow G$$

for some n .

Proof.

(\Rightarrow) As the group is abelian, for $G = \langle a_1, \dots, a_n \rangle$, we can represent an element g uniquely as

$$g = a_1^{p_1} \cdots a_n^{p_n}$$

where $p_i \in \mathbb{Z}$, $i = 1, \dots, n$. Therefore we can explicitly write down the surjective homomorphism

$$\varphi : \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}} \twoheadrightarrow G \quad \text{by} \quad \varphi(p_1, \dots, p_n) = a_1^{p_1} \cdots a_n^{p_n} = g$$

as desired.

(\Leftarrow) By the universal property of $\mathbb{Z}^{\oplus n}$ we have the following diagram that commutes:

$$\begin{array}{ccc} \mathbb{Z}^{\oplus n} & \xrightarrow{\exists! \varphi} & G \\ \uparrow j & \nearrow f & \\ \{1, \dots, n\} & & \end{array} \quad (*)$$

To prove, it suffices to "replace" the set $\{1, \dots, n\}$ by a subset of G .

$$\begin{array}{ccccc} & & \mathbb{Z}^{\oplus n} & \xrightarrow{\exists! \varphi} & G \\ & \nearrow j & \uparrow \tilde{j} & \nearrow i & \\ \{1, \dots, n\} & \xrightarrow{f} & A & & \end{array}$$

By the diagram (*), we have $i \circ f = \varphi \circ j$. It is a fast check that the diagram formed by \tilde{j} , i and φ commutes. Finally since A is a finite set and $\text{im } \varphi = G$, it follows by definition that G is finitely generated. ■

Problem II.6.14. Let ϕ be the Euler's ϕ -function. Prove that for $n \in \mathbb{N}$,

$$\sum_{m>0, m|n} \phi(m) = n.$$

Proof. Let $\langle x \rangle = C_n$. We have the trivial equation

$$\sum_{g \in C_n} 1 = n$$

Now note that every element in C_n generates a cyclic subgroup. To establish the result, we show that for every $d > 0$ that is a divisor of n , the subgroup of order d is *unique*, i.e. the unique subgroup is given by

$$\langle x^{n/d} \rangle = \{g \in G : g^d = 1\}$$

Indeed, if $g = x^{kn/d}$ for some positive integer k , then $g^d = x^{kn} = 1$. Conversely, if $g^d = 1$, then we have $g = x^m$ for some m since x is a generator. But this means that $x^{md} = 1$, and this implies $n|md$. Hence we have

$$g = x^m = x^{n/d \cdot dm/n} = x^{n/d} \in \langle x^{n/d} \rangle$$

as desired.

Now we count the generators of each subgroup of C_n , which is $\phi(d)$ for every d that is a divisor of n . Since every element in C_n generates a cyclic subgroup C_d , the sum of generator along each subgroup is exactly n , namely

$$\sum_{g \in C_n} 1 = \sum_{m: m|n} \phi(m) = n$$

which proved the assertion. ■

Problem II.6.15. Prove that if $\varphi : G \rightarrow G'$ has a left inverse, then φ is a monomorphism.

Proof. If $a, b \in G$ are distinct elements that satisfies $\varphi(a) = \varphi(b)$, then having left inverse means there exists a homomorphism ψ such that $\psi \circ \varphi = id_G$. Then we would have $\psi \circ \varphi(a) = \psi \circ \varphi(b)$, which means $a = b$, a contradiction. ■

II.7

Problem II.7.3. Verify that the equivalent conditions for normality given in §7.1 are indeed equivalent.

Proof. Let $g \in G$ be fixed.

- $(gng^{-1} \in N \Rightarrow gNg^{-1} \subseteq N)$ is clear.
 - $(gNg^{-1} \subseteq N \Rightarrow gNg^{-1} = N)$: For $n \in N$, there is an element $g^{-1}ng \in N$ by normality, so $g(g^{-1}ng)g^{-1} = n$, showing that $gNg^{-1} \supseteq N$.
 - $(gNg^{-1} = N \Rightarrow gN \subseteq Ng)$: For $h \in gN$, there is $h = gn$ for some $n \in N$. By normality of N , there is some $n' \in N$ such that $gng^{-1} = n'$, or $gn = n'g$. Hence $h = n'g$, therefore $h \in Ng$.
 - $(gN \subseteq Ng \Rightarrow gN = Ng)$: If $gN \subseteq Ng$, then we also have $g^{-1}N \subseteq Ng^{-1}$, which is $Ng \subseteq gN$.
 - $(gN = Ng \Rightarrow gng^{-1} \in N)$: If $gn = n'g$, then $gng^{-1} = n'$. Since N is a subgroup, $gng^{-1} \in N$.
-

Problem II.7.7. Let n be a positive integer. Let $H \subset G$ be the subgroup generated by all elements of order n in G . Prove that H is normal.

Proof. For $a \in H, g \in G$, since $a^n = e$,

$$(gag^{-1})^n = ga^n g^{-1} = e$$

we have $gag^{-1} \in H$, hence normal. ■

Problem II.7.11. Prove that the commutator subgroup $[G, G]$ is normal, and the quotient $G/[G, G]$ is commutative.

Proof. Observe

$$gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = xyx^{-1}y^{-1} \in [G, G]$$

for $x = gag^{-1}, y = gbg^{-1}$. The quotient is commutative since $aba^{-1}b^{-1}[G, G] = [G, G]$ implies $ab[G, G] = ba[G, G]$. ■

II.8

Problem II.8.7. Let $(A|\mathcal{R}), (A'|\mathcal{R}')$, be the presentation for groups G, G' , respectively, and assume that A and A' are disjoint. Prove that

$$G * G' := (A \cup A' \mid \mathcal{R} \cup \mathcal{R}')$$

satisfies the universal property for the coproduct of G and G' in \mathbf{Grp} .

Proof. Write $H = \mathcal{R} \cup \mathcal{R}'$. Let us construct a homomorphism from G to $G * G'$. As $G = F(A)/R$, by the universal property of quotient we have a commutative diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{f} & G * G' \\ & \searrow \pi & \nearrow \exists! \varphi_1 \\ & F(A)/\mathcal{R} & \end{array}$$

In particular, we let f be an quotient map, i.e. $f(w) = wH$. Then naturally we have $\varphi_1(w\mathcal{R}) = wH$. Similarly, for G' we have another homomorphism $\varphi_2(v\mathcal{R}') = vH$.

Now it suffices to check the universal property. For every homomorphism that maps G and G' to a group K , which we call them f_1 and f_2 , we can define $\phi : G * G' \rightarrow K$ by

$$\phi(wH) = \prod_{i=1}^{|w|} (f_1(w_i\mathcal{R})\chi_{F(A)}(w_i) + f_2(w_i\mathcal{R}')\chi_{F(A')}(w_i))$$

where $w = w_1 \cdots w_n$, χ is the indicator function. The commutative of the coproduct diagram is clear, and ϕ is clearly a homomorphism since we can clearly combine two finite product to one. ■

Problem II.8.13. Let G be a finite group, and assume $|G|$ is odd. Prove that every element of G is a square.

Proof. Let $|G| = 2n - 1$, $n \in \mathbb{N}$. For every $g \in G$, we have

$$g = g \cdot g^{2n-1} = g^{2n} = (g^n)^2$$

which implies that every element in G is a square. ■

Problem II.8.13. Generalize the result of II.8.13: if G is a group of order n and k is an integer relatively prime to n , then the function $G \rightarrow G, g \rightarrow g^k$ is surjective.

Proof. By the prime condition, we can apply Bezout's identity, namely there exists integers a, b such that $an + bk = 1$. Then for every $g \in G$, we have

$$g = g \cdot g^{-an} = g^{1-an} = g^{bk} = (g^b)^k$$

which implies that every element in G is a k -power of some element in G . ■

Problem II.8.17. Assume that G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p .

Proof. We proceed by induction. Clearly if $|G| = 1$ then the statement is true. Now suppose for all abelian group with order less than n , we can find a element whose order is a prime and a divisor of G . Then for any group G that has order n , consider an element $g \in G$, and consider the subgroup generated by g , $H = \langle g \rangle$.

Clearly H is cyclic, so we can find a element $g^{|g|/q}$ of order q where q is a prime since

$$1 = g^{|g|} = (g^{|g|/q})^q$$

provided that $q \mid |g|$. Now if $q = p$, then we are done; otherwise, we replace G with $G/\langle h \rangle$, where $h = g^{|g|/q}$ (note that all subgroups are normal since G is abelian). Now this quotient has order less than n , and by induction, we can find an element of order p in it, which we call it $m\langle h \rangle$. Finally the element mh^q has order p , since

$$(mh^q)^p = m^p g^{p|g|} = 1$$

Note that the commutative is used here. ■

Problem II.8.20. Assume that G is a finite abelian group, and let d be a divisor of $|G|$. Prove that there exists a subgroup $H \subseteq G$ of order d .

Proof. We proceed by induction. Clearly if $|G| = 1$ then the statement is true. Now suppose for all abelian group with order less than n , we can find a subgroup whose order is a divisor of $|G|$. Then if $|G| = n$, then by II.8.18, we have an element in G that is of order p , where p is a prime and a divisor of d . If $p = d$, then we are done. Otherwise, we consider the quotient $G/\langle p \rangle$. This group has order $|G|/p$, and by induction hypothesis, we can find a subgroup H in the quotient that is of order d/p . Now we claim that the set

$$H' = \{gp^n : n \in \{0, \dots, p-1\}, g\langle p \rangle \in H\}$$

is a subgroup of order d . It is indeed a subgroup since for $g, h \in H'$,

$$gh^{-1} = ap^kb^{-1}p^{-l} = ab^{-1}p^{k-l} \in H'$$

for some a, b that is a coset representative ($ab^{-1}\langle p \rangle \in H$ since H is a subgroup). As the cosets are disjoint, there are precisely $p \cdot d/p = d$ elements in H' , proving the assertion. ■

Problem II.8.21. Let H, K be subgroups of a group G . Construct a bijection between the set of cosets hK with $h \in H$ and the set of left-cosets of $H \cap K$ in H . If H and K are finite, prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Proof. The map $hK \leftrightarrow h(K \cap H), h \in H$ is a bijection: it is well-defined since for $g, h \in H$, $gK = hK$ implies $gh^{-1} \in K$, and since $g, h \in H$, $gh^{-1} \in H \cap K$ and hence $g(H \cap K) = h(H \cap K)$. It is injective by reversing the above argument, and surjective by construction.

$$\{hK : h \in H\} \longleftrightarrow \{h(H \cap K) : h \in H\}$$

Now the set on the left has $|HK|/|H|$ elements in total, and the set on the right has $|H|/|H \cap K|$. A simple rearrangement gives the result. ■

Problem II.8.22. Let $\varphi : G \rightarrow G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\text{im } \varphi$. Prove that G'/N satisfies the universal property of $\text{coker } \varphi$ in Grp .

Proof. By universal property of quotient, for every homomorphism $\alpha : G' \rightarrow L$, the homomorphism $\bar{\alpha} : G'/N \rightarrow L$ exists and is unique. Now it suffices to check the universal property of cokernel. For any $\alpha : G' \rightarrow L$ such that $\alpha \circ \varphi = 0$, define $\bar{\alpha}(gN) = \alpha(g)$. We need to check that this is well defined. If $\bar{\alpha}(gN) = \bar{\alpha}(hN)$ but $\alpha(g) \neq \alpha(h)$, then $gh^{-1} \notin \ker \alpha$. However since $\alpha \circ \varphi = 0$, $\text{im } \varphi \subseteq \ker \alpha$. By noting that N is normal and minimal, we have

$$\ker \alpha \supseteq N \ni gh^{-1}$$

since $gN = hN$. This is a contradiction, therefore $\alpha(g) = \alpha(h)$, showing the well-definedness of $\bar{\alpha}$. Then

$$\bar{\alpha}(\pi(\varphi(g))) = \bar{\alpha}(N) = \alpha(e) = e_L$$

for all $g \in G$. This shows $\bar{\alpha} \circ \pi \circ \varphi = 0$, and the assertion is proved. ■

Problem II.8.24. Show that epimorphisms in Grp do not necessarily have right-inverses.

Proof. Let

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_2, \quad \varphi(x) = x \pmod{2}$$

this map has no right inverses as any homomorphism from \mathbb{Z}_2 to \mathbb{Z} can only be the identity map. ■

II.9

Problem II.9.7. Prove that stabilizers are indeed subgroups.

Proof. Assume G acts on A , and pick $a \in A$. For $g, h \in \text{Stab}_G(a)$, we have

$$gh^{-1}a = g(h(h^{-1}a)) = ga = a$$

as required. ■

Problem II.9.11. Let G be a finite group, and let H be a subgroup of index p , where p is the smallest prime dividing $|G|$. Prove that H is normal in G .

Proof. We consider the left-multiplication action of G on the left cosets of H , which is $g \cdot hH = ghH$. This induces a homomorphism $\varphi : G \rightarrow S_p$, whose kernel includes H since

$$\text{if } g \in \ker \varphi, \text{ then } aH = gaH \forall a \in G \Rightarrow g = gH \Rightarrow g \in H.$$

Then $G/\ker \varphi \cong \text{im } \varphi$, so $G/\ker \varphi$ is a subgroup of S_p , therefore it has order dividing $p!$. However by Lagrange, such order also divides $|G|$, and hence must be divisible by p , so $|G/\ker \varphi| = p$. Finally

$$p = [G : H] = [G : \ker \varphi][\ker \varphi : H] = p[\ker \varphi : H]$$

which leads to $[\ker \varphi : H] = 1$. Since $\ker \varphi \subseteq H$, $\ker \varphi = H$ by index consideration, proving the assertion. ■

Problem II.9.12. Let G be a group, and let $H \subseteq G$ be a subgroup of index n . Prove that H contains a subgroup K that is normal in G and such that $[G : K]$ divides the gcd of $|G|$ and $n!$. (In particular, $[G : K] \leq n!$.)

Proof. Following the same pattern from II.9.11, consider the left-multiplication action of G on the left cosets of H , which is $g \cdot hH = ghH$. This induces a homomorphism $\varphi : G \rightarrow S_n$ (as there are n left cosets), whose kernel includes H since

$$\text{if } g \in \ker \varphi, \text{ then } aH = gaH \forall a \in G \Rightarrow g = gH \Rightarrow g \in H.$$

Define $K = \ker \varphi$. Then $G/K \cong \text{im } \varphi$, so G/K is a subgroup of S_n , therefore it has order dividing $n!$. By Lagrange, such order also divides $|G|$, so we've found the required K . ■

Problem II.9.13. Prove 'by hand' that that for all subgroups H of a group G and $\forall g \in G$, G/H and $G/(gHg^{-1})$ (endowed with the action of G by left-multiplication) are isomorphic in $G\text{-Set}$.

Proof. We want to find a *bijection* function $\varphi : G/H \rightarrow G/gHg^{-1}$ such that the diagram

$$\begin{array}{ccc} G \times G/H & \xrightarrow{id_G \times \varphi} & G \times G/gHg^{-1} \\ \downarrow \rho & & \downarrow \rho' \\ G/H & \xrightarrow{\varphi} & G/gHg^{-1} \end{array}$$

commutes. Indeed the most natural map would be $\varphi(xH) = (gxg^{-1})gHg^{-1}$. We check that this is well-defined; if $aH = bH$, then $gaHg^{-1} = gbHg^{-1}$ clearly. We now check that this is a bijection, by explicitly give the inverse

$$\phi : G/gHg^{-1} \rightarrow G/H, \quad \phi(xgHg^{-1}) = (g^{-1}xg)H$$

so $\varphi \circ \phi = id$. Therefore G/H and $G/(gHg^{-1})$ are isomorphic in $G\text{-Set}$. Note that if we assume $\varphi(xH) = xgHg^{-1}$, then H would need to be normal in order to be well-defined. ■

Problem II.9.17. Consider G as a G -set, by acting with left-multiplication. Prove that $\text{Aut}_{G\text{-Set}(G)} \cong G$.

Proof. The set of automorphisms on $G - \text{Set}(G)$ are bijections that satisfies $g\varphi(h) = \varphi(gh)$. In particular we can define

$$\varphi_g(h) = g^{-1}h$$

this is clearly a bijection and forms a group structure by $\varphi_g\varphi_h = \varphi_{gh}$. We now consider the map $\psi : \text{Aut}_{G\text{-Set}(G)} \rightarrow G$ by $\psi(\varphi_g) = g$. We claim that this is an isomorphism. Indeed, its kernel is precisely φ_e , which is the identity of $\text{Aut}_{G\text{-Set}(G)}$. The map is clearly surjective, and it is an homomorphism by construction. Therefore $\text{Aut}_{G\text{-Set}(G)} \cong G$. ■

Chapter III

Rings and modules

Unless otherwise specified, in the following $R = (R, +, \cdot)$ denotes an arbitrary ring *with identity* (the book assumes this throughout this book), $0, 1$ denotes the additive and multiplicative identity of R , respectively. In the case of possible confusion, I will use $0_R, 1_R$ instead.

Some description and hints are omitted for simplicity.

III.1

Problem III.1.1. Prove that if $0 = 1$ in a ring R , then R is a zero ring.

Proof. If r is any element in R , then

$$r = r \cdot 1 = r \cdot 0 = 0$$

showing that $R = 0$. ■

Problem III.1.6. Prove that if a and b are nilpotent in R and $ab = ba$, then so is $a + b$.

Proof. If $a^n = 0, b^m = 0$, then

$$(a + b)^{n+m} = a^{n+m} + \binom{n+m-1}{1} a^{n+m-1}b + \dots + b^{n+m}$$

and all terms are zeros since every term either have a^n or b^m . If we do not assume that $ab = ba$, then the statement would be false, for example, in $M_n(\mathbb{Z})$,

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

are nilpotent of degree 3, but $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ is not nilpotent. ■

Problem III.1.7. Prove that $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all prime factors of n .

Proof.

(\Rightarrow) If $[m]^k = [0]$ for some integer k , then this implies $m^k = dn$ for some integer d . Now we write $n = p_1^{a_1} \cdots p_n^{a_n}$, where p_i are primes, and a_i are positive integers. Then

$$m^k = dp_1^{a_1} \cdots p_n^{a_n}$$

and it is clear to see that m must contain each p_i at least once.

(\Leftarrow) If $n = p_1^{a_1} \cdots p_n^{a_n}$ where p_i are primes, and a_i are positive integers, then we can write

$$m = p_1^{b_1} \cdots p_n^{b_n} d$$

where b_i, d are positive integers, and $p_i \nmid d$ for all i . Define

$$f = \text{floor} \left(\max \left\{ \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \right\} \right)$$

then let $r = m^f/n$, which is an integer larger than 0 by the choice of f . Finally

$$m^f = nr = 0 \pmod n$$

showing that m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. ■

Problem III.1.9. Prove Proposition 1.12, that is:

- *The inverse of a two-sided unit is unique;*
- *two-sided units form a group under multiplication.*

Proof. For a two-sided unit v , we have $uv = 1$ and $vw = 1$ for some $u, w \in R$. Then

$$w = 1 \cdot w = uvw = u \cdot 1 = u$$

showing that $w = u$, so the inverse can be uniquely defined as $v^{-1} = u$. Now as the inverse is unique, we can properly define a group structure, using the multiplication from the ring R . ■

Problem III.1.15. Prove that $R[x]$ is a domain if and only if R is a domain.

Proof.

(\Rightarrow) Trivial since $R \subset R[x]$.

(\Leftarrow) Assume the contrary that $R[x]$ is not a domain. Then we can find $f = \sum_{i=0}^n a_i x^i$, $g = \sum_{j=0}^m b_j x^j$, $f \neq 0, g \neq 0$ such that $fg = 0$. Then we would have $a_n b_m = 0$, and since R is a domain, either a_n or b_m is zero. Without loss of generality, we can reduce the case to $f = a_0 \neq 0$. Then by the same argument, we would arrive at $a_0 b_0 = 0$, since all higher terms must be zero. But this contradicts to the assumption that R is a domain, since $f = a_0$ and $g = b_0$ are nonzero. Hence $R[x]$ must be a domain. ■

III.2

Problem III.2.1. Prove that if there is a homomorphism from a zero ring to a ring R , then R is a zero ring.

Proof. If 1_R is the multiplicative identity of R , then for any homomorphism $\varphi : 0 \rightarrow R$,

$$0_R = \varphi(0) = \varphi(1) = 1_R$$

and by III.1.1, R is a zero-ring. ■

Problem III.2.6. Verify the 'extension property' of polynomial ring:

Let $\alpha : R \rightarrow S$ be a fixed ring homomorphism, and let $s \in S$ be an element commuting with $\alpha(r)$ for all $r \in R$. Then there is a unique ring homomorphism $\bar{\alpha} : R[x] \rightarrow S$ extending α and sending x to s .

Proof. Indeed, for $\sum_{i \geq 0} a_i x^i \in R[x]$, we have no choice but to define

$$\bar{\alpha} \left(\sum_{i \geq 0} a_i x^i \right) = \sum_{i \geq 0} \alpha(a_i) s^i \quad (1)$$

so that $\bar{\alpha}(r) = \alpha(r)$ and x sends to s in this map. It is clearly a homomorphism (note that the commutativity of s is used in the proof of $\bar{\alpha}(fg) = \bar{\alpha}(f)\bar{\alpha}(g)$), so it suffices to check that $\bar{\alpha}$ is unique. But it is clear by the fact that any map that extends α and send x to s must have the same value evaluated as in (1). ■

Problem III.2.9. Prove that the center of R is a subring. Moreover, prove that the center of a division ring is a field.

Proof. A subset of a ring S is a subring if it is a subgroup of $(R, +)$, closed under multiplication, and 1 is in it. So we check that:

- it is a subgroup of $(R, +)$: for $a, b \in C$, for all $r \in R$,

$$(a - b)r = ar - br = ra - rb = r(a - b)$$

showing that $a - b \in C$, hence a subgroup;

- closed under multiplication: for $a, b \in C$, for all $r \in R$,

$$abr = a(br) = a(rb) = (ar)b = (ra)b = rab$$

showing that $ab \in C$;

- finally, 1 is in C since $1r = r1$ for all $r \in R$.

Clearly the center forms a commutative ring since for $a, b \in C$, $ab = ba$. Then it follows by definition that a commutative division ring is a field. ■

Problem III.2.10. Prove that the centralizer of a is a subring for every $a \in R$. Prove that the center is the intersection of all its centralizers, and prove that every centralizer of a division ring is a division ring.

Proof. We use the same test as above. Let C_x denotes the centralizer of x .

- It is a subgroup of $(R, +)$: for $a, b \in C_x$,

$$(a - b)x = ax - bx = xa - xb = x(a - b)$$

showing that $a - b \in C_x$, hence a subgroup;

- closed under multiplication: for $a, b \in C_x$,

$$abx = a(bx) = a(xb) = (ax)b = (xa)b = xab$$

showing that $ab \in C_x$;

- finally, 1 is in C_x since $1x = x1$.

It is easy that the center is the intersection of all its centralizers, since such element in the intersection must commute with the whole ring R . Finally, if R is a division ring, then for every element $a \in C_x$, we can show that $a^{-1} \in C_x$:

$$ax = xa \Rightarrow axa^{-1} = x \Rightarrow xa^{-1} = a^{-1}x$$

Therefore every element in C_x has an inverse, and by definition, C_x is a division ring. ■

Problem III.2.11. Prove that a division ring R which consists of p^2 elements where p is a prime, is commutative.

Proof. Suppose the contrary that R is not commutative. Then the center C must be a proper subring, which can only consist of p elements by Lagrange. Now let $r \in R \setminus C$. Then the centralizer of r will contain at least r and C by III.2.10, therefore the centralizer of r must be R itself (again by Lagrange), for every $r \in R \setminus C$. But then the intersection of all centralizer are now R (element of center has centralizer R clearly), which is a contradiction to that C is proper. Therefore R must be commutative, i.e. a field. ■

Problem III.2.12. Consider the inclusion map $\iota : \mathbb{Z} \hookrightarrow \mathbb{Q}$. Describe the cokernel of ι in **Ab** and its cokernel in **Ring**.

Solution. In **Ab**, this is easy: it is just $\mathbb{Q}/\text{im } \iota = \mathbb{Q}/\mathbb{Z}$. However in **Ring**, we notice that for any map $\alpha : \mathbb{Q} \rightarrow F$ that satisfy $\alpha \circ \iota = 0$, we have

$$0_F = \alpha(1) = \alpha \circ \iota(1) = \alpha(1) = 1_F$$

which shows that F must be the zero ring by III.1.1. Now the unique homomorphism $\bar{\alpha} : \text{coker } \iota \rightarrow F$ must also be the zero map, and by the requirement $\bar{\alpha} \circ \pi \circ \iota = 0$, we finally have $\pi \circ \iota = 0$, and by the same argument as above, we have that the codomain of π is the zero ring, i.e. $\text{coker } \iota = 0$. ■

III.3

Problem III.3.2. Let $\varphi : R \rightarrow S$ be a ring homomorphism, and let J be an ideal of S . Prove that $\varphi^{-1}(J)$ is an ideal.

Proof. The ideal is clearly nonempty, so it suffices to check that $\varphi^{-1}(J)$ is a additive subgroup and satisfies the absorption property. For $x, y \in \varphi^{-1}(J)$, we have $\varphi(x), \varphi(y) \in J$, so $\varphi(x) - \varphi(y) = \varphi(x - y) \in J$, therefore $x - y \in \varphi^{-1}(J)$, showing that it is a subgroup of $(R, +)$.

Now for any $r \in R, a \in \varphi^{-1}(J)$, we have $\varphi(a) \in J$, so $\varphi(r)\varphi(a) = \varphi(ra) \in J$, and hence $ra \in \varphi^{-1}(J)$, showing the left-absorption property. The right case is the same. ■

Problem III.3.3. Let $\varphi : R \rightarrow S$ be a ring homomorphism, and let J be an ideal of R .

- Show that $\varphi(J)$ need not be an ideal of S .
- Assume that φ is surjective; then prove that $\varphi(J)$ is an ideal of S .
- Assume that φ is surjective, and let $I = \ker \varphi$. Let $\bar{J} = \varphi(J)$. Prove that

$$\frac{R/I}{\bar{J}} \cong \frac{R}{I + J}.$$

Proof. Let $\varphi : \mathbb{Z} \hookrightarrow \mathbb{R}$ be inclusion (and clearly a homomorphism). Then every ideal of \mathbb{Z} will be directly transformed into \mathbb{R} . But since \mathbb{R} is a field, by III.3.8 (which will be proved later) the possible ideal of \mathbb{R} are only $\{0\}$ and \mathbb{R} itself, so the image of a homomorphism need not to be an ideal.

However, If φ is surjective, Then $\varphi(J)$ is indeed an ideal: if $\varphi(x), \varphi(y) \in \varphi(J)$, then so is $\varphi(x) - \varphi(y) = \varphi(x - y) \in \varphi(J)$. The absorption property is also true since $\varphi(r)\varphi(x) = \varphi(rx) \in \varphi(J)$.

Finally, we consider the homomorphism

$$\phi : R/I \rightarrow R/(I + J), \quad \phi(a + I) = a + I + J$$

ϕ is clearly a surjective homomorphism, and by first isomorphism theorem

$$\frac{R/I}{\ker \phi} \cong \frac{R}{I+J}$$

so it remains to solve $\ker \phi$, which is

$$\begin{aligned} \ker \phi &= \{a + I : a + I + J = I + J\} \\ &= \{a + b + I : a \in I, b \in J\} \\ &= \{b + I : b \in J\} \\ &= \{\varphi(b) \in S : b \in J\} \quad (\text{regarding } R/I \text{ as } S) \\ &= \varphi(J) = \bar{J} \end{aligned}$$

therefore

$$\frac{R/I}{\bar{J}} \cong \frac{R}{I+J}$$

as required. ■

Problem III.3.7. Let R be a ring, and let $a \in R$. Prove that Ra is a left-ideal of R and aR is a right-ideal of R . Prove that a is a left-, resp. right-, unit if and only if $R = aR$, resp. $R = Ra$.

Proof. We prove only the left-ideal case since the same argument holds for right-ideal case. Ra is a subgroup of $(R, +)$ since for $ra, sa \in Ra$, $ra - sa = (r - s)a \in Ra$. The absorption property follows easily since $rsa = (rs)a \in Ra$.

If a is a right unit, then there exists u such that $ua = 1$. Then 1 is contained in Ra , and since for all $r \in R$, $r \cdot 1 \in Ra$, we conclude that $R = Ra$. ■

Problem III.3.8. Prove that R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R .

In particular, a commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R .

Proof.

(\Rightarrow) If a nonzero element a is in the left-ideal I , then so is 1 since

$$1 = a^{-1}a \in I \text{ by definition}$$

Therefore any nonzero left-ideals are automatically R itself. The right-ideal case is the same.

(\Leftarrow) If a nonzero element a does not have a left inverse, then aR would be a proper right-ideal by III.3.7. Therefore all elements must have left(and hence right) inverse. ■

Problem III.3.10. Let $\varphi : k \rightarrow R$ be a ring homomorphism, where k is a field and R is a nonzero ring. Prove that φ is *injective*.

Proof. φ is injective if and only if $\ker \varphi = \{0\}$ by Proposition III.2.4. Also, the ideals of k are only $\{0\}$ and k by III.3.8. If $\ker \varphi = \{0\}$ then there is nothing to prove, so let $\ker \varphi = k$. But this means that $\varphi = 0$, so we have

$$1_R = \varphi(1) = 0 = \varphi(0) = 0_R$$

and by III.1.1, R is a zero ring, a contradiction to the hypothesis. Therefore $\ker \varphi = \{0\}$, showing that φ is injective. ■

Problem III.3.12. Let R be a *commutative* ring. Prove that the set of nilpotent elements forms an ideal of R . This ideal is called the *nilradical* of R .

Proof. From III.1.6 we already know that it forms a subgroup of $(R, +)$ by replacing b with $-b$, so it remains to check that it is an ideal. Let I be such ideal. If $a \in R, r \in I$ and $r^n = 0$, then since

$$(ar)^n \stackrel{!}{=} a^n r^n = 0$$

in which $!$ is where commutative is used. Therefore $ar \in I$, proving the absorption property.

For an counter-example where R is not commutative, simply consider the example of III.1.6: it is not even a subgroup of $(R, +)$. ■

Problem III.3.13. Let R be a commutative ring, and let N be its nilradical. Prove that R/N contains no nonzero nilpotent elements. Such a ring is said to be *reduced*.

Proof. Pick an element $a \in R \setminus N$. Then for every integer $n > 0$,

$$(a + N)^n = a^n + \binom{n}{1} a^{n-1} N + \cdots + N^n = a^n + N$$

Since a is not nilpotent, $a^n \neq 0$ for every n , showing that $a + N$ is not nilpotent for $a \in R \setminus N$. ■

III.4

Problem III.4.1. Let R be a ring, and let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals of R . We let

$$\sum_{\alpha \in A} I_\alpha := \left\{ \sum_{\alpha \in A} r_\alpha \text{ such that } r_\alpha \in I_\alpha \text{ and } r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Prove that $\{I_\alpha\}_{\alpha \in A}$ is an ideal of R and that it is the smallest ideal containing all of the ideals I_α .

Proof. We only consider the case when $A = \{1, 2\}$: Any other A follows the same exact argument.

Let $I = I_1 + I_2$. I is a subgroup of $(R, +)$: the two elements in I can be represented as $r_1 + r_2$ and $r'_1 + r'_2$, and clearly $(r_1 - r'_1) + (r_2 - r'_2)$ is in I . The absorption property is also clear, since $r(r_1 + r_2) = (rr_1 + rr_2) \in I$.

Now it suffice to show that I is minimal. For every ideal that contains I_1 and I_2 , they must also contain $r_1 + r_2$ for $r_1 \in I_1$ and $r_2 \in I_2$, since ideal is a subgroup of $(R, +)$. Therefore every such ideal must also contain I , proving the minimality of I . ■

Problem III.4.2. Prove that the homomorphic image of a Noetherian ring is Noetherian.

Proof. Let R be Noetherian, S be any ring, $\varphi : R \rightarrow S$ be a surjective ring homomorphism. Let J be an ideal of S . By III.3.2, the preimage is an ideal, which we call $I = \langle a_1, \dots, a_n \rangle$. We claim that $J = \langle \varphi(a_1), \dots, \varphi(a_n) \rangle$, so every finitely generated ideal will map to a finitely generated ideal, proving that S is Noetherian.

Indeed, since $a_i \in \varphi^{-1}(J)$, $\varphi(a_i) \in J$ for $i = 1, \dots, n$, so $\langle \varphi(a_1), \dots, \varphi(a_n) \rangle \subseteq J$. On the other hand, for an element $j \in J$, there exists $i \in R$ such that $\varphi(i) = j$ by surjectivity, therefore $i \in I$, so i is generated by elements a_1, \dots, a_n , i.e. $i = r_1 a_1 + \dots + r_n a_n$. Then since φ is a homomorphism,

$$\varphi(i) = j = \varphi(r_1 a_1 + \dots + r_n a_n) = s_1 \varphi(a_1) + \dots + s_n \varphi(a_n)$$

so $J \subseteq \langle \varphi(a_1), \dots, \varphi(a_n) \rangle$, and the claim is proved. ■

Problem III.4.3. Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

Proof. Assume that $(f) = (2, x)$. Then there is some $q \in \mathbb{Z}[x]$ such that $fq = 2$. Then f, q are constant and f must be 2 since 1 is not in it. But we also have $fg = x$ for some $g \in \mathbb{Z}[x]$, and there are no possible choice of g such that $2g = x$. Hence $(2, x)$ is not principal. ■

Problem III.4.4. Prove that if k is a field, then $k[x]$ is a PID.

Proof. Let I be any ideal of $k[x]$. If $I = (0)$, then there is nothing to prove. Otherwise, there is some polynomial $f \in I$ that has minimal degree in I and is monic (since you can do scalar division). We claim that $I = (f)$. Indeed, for $g \in I$, we can use division algorithm to write

$$g(x) = f(x)q(x) + r(x)$$

where $\deg r(x) < \deg f(x)$. Since $k[x]$ is a subgroup, $r = g - fq \in I$, and by the minimality of f , $r(x) = 0$, so every element of I can be written as $g(x)f(x)$ for some $g \in k[x]$, showing that $k[x]$ is a PID. ■

Problem III.4.5. Let I, J be ideals in a commutative ring R , such that $I + J = (1)$. Prove that $IJ = I \cap J$.

Proof. If $x \in IJ$, then it can be represented as ij for some $i \in I, j \in J$, and by the property of ideal, $ji \in I, ij \in J$, so $ij \in I \cap J$. Conversely, we have

$$I \cap J = (I \cap J)(1) = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subseteq IJ + IJ = IJ$$

showing the identity. ■

Problem III.4.7. Let $R = k$ be a field. Prove that every nonzero (principle) ideal in $k[x]$ is generated by a unique *monic* polynomial.

Proof. From III.4.4 we already know that every ideal is generated by a single polynomial f . Since k is a field, we can do division, so there is a monic polynomial $f(x)/a$ where a is the coefficient of the largest degree in f . Then it's trivial that $(f) = (f/a)$. ■

Problem III.4.11. Let R be a commutative ring, $a \in R$, and $f_1(x), \dots, f_r(x) \in R[x]$.

- Prove the equality of ideals

$$(f_1(x), \dots, f_r(x), x - a) = (f_1(a), \dots, f_r(a), x - a).$$

- Prove the useful substitution trick

$$\frac{R[x]}{(f_1(x), \dots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \dots, f_r(a))}$$

Proof. We consider only the case $k = 1$; the other cases are just extending the same argument. We are required to prove that

$$(f(x), x - a) = (f(a), x - a)$$

For $f(x)$, we can apply division algorithm to get

$$f(x) = q(x)(x - a) + r$$

where $q(x) \in R[x], r \in R$. By plug in $x = a$, we obtain $r = f(a)$. Therefore $f(x)$ is generated by $f(a)$ and $(x - a)$, showing $f(x) \in (f(a), x - a)$. On the other hand, note the division algorithm also implies

$$f(a) = f(x) - q(x)(x - a) \in (f(x), x - a)$$

therefore $f(a) \in (f(x), x - a)$, so $(f(x), x - a) = (f(a), x - a)$. Now since $R[x]/(x - a) \cong R$, by III.3.3

$$\frac{R}{\varphi(J)} \cong \frac{R[x]}{\ker \varphi + J}$$

for an ideal $J \in R[x]$, $\varphi : R[x] \rightarrow R$ a surjective homomorphism. It is clear that how should we choose these: by taking

$$J = (f_1(x), \dots, f_r(x)), \quad \varphi(f(x)) = f(a)$$

we have

$$\frac{R}{(f_1(a), \dots, f_r(a))} \cong \frac{R[x]}{(f_1(x), \dots, f_r(x), x - a)}$$

as desired (note that φ is surjective). ■

Problem III.4.13. Let R be an integral domain. For all $k = 1, \dots, n$, prove that (x_1, \dots, x_k) is prime in $R[x_1, \dots, x_n]$.

Proof. We proceed by induction. For the case $k = 1$, we have

$$\frac{R[x]}{(x)} \cong R \quad (\text{p.p.151})$$

and since R is a domain, it follows by definition that (x) is a prime ideal. Suppose that for $k < n$, the argument holds. Then for $k = n$, choose

$$J = (x_1, \dots, x_{n-1}), \quad \varphi : R[x_1, \dots, x_n] \hookrightarrow R[x_1, \dots, x_{n-1}]$$

where φ is the inclusion map and $\ker \varphi = (x_n)$. Then by III.3.3

$$\frac{R[x_1, \dots, x_n]/(x_n)}{(x_1, \dots, x_{n-1})} \cong \frac{R[x_1, \dots, x_n]}{(x_1, \dots, x_{n-1}) + (x_n)}$$

which simplifies to

$$\frac{R[x_1, \dots, x_{n-1}]}{(x_1, \dots, x_{n-1})} \cong \frac{R[x_1, \dots, x_n]}{(x_1, \dots, x_n)}$$

By induction hypothesis, the quotient on the left is a domain since (x_1, \dots, x_{n-1}) is a prime ideal, therefore by definition, (x_1, \dots, x_n) is a prime ideal. ■

Problem III.4.16. Let R be a commutative ring, and let P be a prime ideal of R . Suppose 0 is the only zero-divisor of R contained in P . Prove that R is an integral domain.

Proof. Let $a, b \in R$ such that $ab = 0$. Then since $0 \in P$, $ab \in P$, so either $a \in P$ or $b \in P$. Without loss of generality, let $a \in P$. If $a = 0$, then we are done; otherwise, $a \neq 0$, and since $ab = 0$, we must have $b = 0$ as a is not a zero divisor (0 is the only zero-divisor in P). In both cases, we show that $ab = 0$ implies $a = 0$ or $b = 0$, showing that R is a domain. ■

Problem III.4.18. Let R be a commutative ring, and let N be its nilradical (III.3.12). Prove that N is contained in every prime ideal of R .

Proof. Let $x^n = 0$ for some positive integer n , and P a prime ideal. Then since $0 \in P$, we have

$$P \ni 0 = x^n = x \cdot x^{n-1}$$

By the property of prime ideal, either $x \in P$ or $x^{n-1} \in P$. If the former case is true, then we are done; else, we can reduce to the case where either $x \in P$ or $x^{n-2} \in P$. By continuing this process, we will arrive at either $x \in P$ or $x \in P$, showing that in any cases, $x \in P$. Therefore all nilpotent elements are in P , proving the statement. ■

Problem III.4.21. Let k be an algebraic closed field, and let $I \subseteq k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$.

Proof.

(\Leftarrow) We have

$$\frac{k[x]}{(x - c)} \cong k \quad (\text{p.p.151})$$

and since k is a field, it follows by definition that $(x - c)$ is maximal.

(\Rightarrow) Let J be a maximal ideal. By III.4.4, $k[x]$ is a PID, hence every ideal is being generated by a single *monic* polynomial $f(x) \in k[x]$ (III.4.7). Since k is algebraic closed, we can write $f(x) = q(x)(x - c)$ for some $q(x) \in k[x]$, $c \in k$. Then

$$J = (f(x)) = (q(x)(x - c)) \subseteq (x - c)$$

and by Proposition III.4.11, either $J = (x - c)$ or $J = k[x]$. The latter case could not happen since the maximal can not be $k[x]$ itself, therefore $J = (x - c)$, as desired. ■

In the following, let M be a (left-)module over R .

III.5

Problem III.5.2. Prove claim 5.1.

Proof. Let $\sigma : R \rightarrow \text{End}_{\text{Ab}}(M)$ be a ring homomorphism and $\rho : R \times M \rightarrow M$ a function. We verify the following properties:

- $\rho(r, m + n) = \rho(r, m) + \rho(r, n)$.

Note that $\sigma(r)$ is a endomorphism on M . Then

$$\rho(r, m + n) = \sigma(r)(m + n) = \sigma(r)(m) + \sigma(r)(n) = \rho(r, m) + \rho(r, n)$$

- $\rho(r + s, m) = \rho(r, m) + \rho(s, m)$.

$$\rho(r + s, m) = \sigma(r + s)(m) = \sigma(r)(m) + \sigma(s)(m) = \rho(r, m) + \rho(s, m)$$

- $\rho(rs, m) = \rho(r, \rho(s, m))$.

$$\rho(rs, m) = \sigma(rs)(m) = \sigma(r)\sigma(s)(m) = \sigma(r)\rho(s, m) = \rho(r, \rho(s, m))$$

- $\rho(1, m) = m$.

$$\rho(1, m) = \sigma(1)(m) = 1(m) = m$$

■

Problem III.5.3. Prove that $0 \cdot m = 0$ and that $(-1) \cdot m = -m$ for all $m \in M$.

Proof. Since $0m = (0 + 0)m = 0m + 0m$, $0m = 0$. Since $0 = 0m = (-1 + 1)m = (-1)m + m$, $(-1)m = -m$. ■

Problem III.5.11. Let R be commutative, and let M be an R -module. Prove that there is a natural bijection between the set of $R[x]$ -module structures on M (extending the given R -module structure) and $\text{End}_{R\text{-Mod}}(M)$.

Proof. If $f \in \text{End}_{R\text{-Mod}}(M)$, then we have to show that there are some suitable maps

$$\begin{aligned} R[x] \times M &\rightarrow M \\ (f(x), m) &\rightarrow ? \end{aligned}$$

that makes M into a $R[x]$ -module. We consider $(g(x), m) \rightarrow g(f)(m)$, where if $g(x) = \sum_i a_i x^i$, then

$$\sigma(f, m) = \sum_i a_i f^i(m) \text{ where } f^i = \underbrace{f \circ \cdots \circ f}_i \text{ } i \text{ times}$$

We can easily check by definition that M is a $R[x]$ -module. Conversely, if M is a $R[x]$ -module, then define $f(m) = xm$. Then f is indeed an endomorphism (note that the commutativity of R ensures that $rxm = xrm$ for $r \in R$, so f is an endomorphism), proving the statement. ■

Problem III.5.12. Let M, N be R -modules, and let $\varphi : M \rightarrow N$ be a homomorphism of R -modules which has a inverse (therefore a bijection). Prove that φ^{-1} is also a homomorphism of R -modules. Conclude that a bijective R -module homomorphism is a R -module isomorphism.

Proof. Since

$$\varphi(\varphi^{-1}(m) + \varphi^{-1}(n)) = m + n = \varphi(\varphi^{-1}(m + n))$$

we have $\varphi^{-1}(m) + \varphi^{-1}(n) = \varphi^{-1}(m + n)$. And

$$\varphi(r\varphi^{-1}(m)) = r\varphi(\varphi^{-1}(m)) = rm = \varphi(\varphi^{-1}(rm))$$

so $r\varphi^{-1}(m) = \varphi^{-1}(rm)$ indeed. ■

Problem III.5.14. Prove Proposition 5.18, that is:

Let N, P be submodules of an R -module M . Then

- $N + P$ is a submodule of M ;
- $N \cap P$ is a submodule of P , and

$$\frac{N + P}{N} \cong \frac{P}{N \cap P}.$$

Proof. Every element of $N + P$ can be written as $n + p$ where $n \in N, p \in P$. Then it is clear that $r(n + p) = rn + rp \in N + P$ for $r \in M$. For the intersection $N \cap P$, it is also clear that for $p \in P, n \in N \cap P, pr \in N$ since $r \in N$, and $pr \in P$ since $p \in P$.

The proof for the second isomorphism theorem follows exactly the same as in groups (Proposition II.8.11). Consider the homomorphism

$$\varphi : P \rightarrow \frac{N + P}{N}, \quad \varphi(p) = pN$$

it is surjective since for every $(n + p)N$, there is a corresponding p . Then

$$\ker \varphi = \{p \in P : p \in N\} = P \cap N$$

finally it follows by first isomorphism theorem that

$$\frac{N + P}{N} \cong \frac{P}{N \cap P}.$$

■

III.6

Problem III.6.1. Prove Claim 6.3, that is, $F^R(A) \cong R^{\oplus A}$.

Proof. Observe that every element in $R^{\oplus A}$ can be uniquely written as

$$\sum_{a \in A} r_a \chi(a)$$

where $\chi(a) = \chi_a(x)$, the indicator function of a , and $r_a \in R$ for $a \in A$. Then it suffices to check the universal property of free modules: given a function $f : A \rightarrow M$ where M is a module, we show that the following diagram

$$\begin{array}{ccc} R^{\oplus A} & \xrightarrow{\exists! \varphi} & M \\ \chi \uparrow & \nearrow f & \\ A & & \end{array}$$

commutes. Indeed, we define

$$\varphi \left(\sum_{a \in A} r_a \chi(a) \right) = \sum_{a \in A} r_a f(a)$$

then the diagram clearly commutes (and is unique). Finally, φ is a R -Mod homomorphism since

$$\begin{aligned} \varphi \left(\sum_{a \in A} r_a \chi(a) \right) + \varphi \left(\sum_{a \in A} r'_a \chi(a) \right) &= \sum_{a \in A} r_a f(a) + \sum_{a \in A} r'_a f(a) \stackrel{\checkmark}{=} \sum_{a \in A} (r_a + r'_a) f(a) \\ &= \varphi \left(\sum_{a \in A} (r_a + r'_a) \chi(a) \right) = \varphi \left(\sum_{a \in A} r_a \chi(a) + \sum_{a \in A} r'_a \chi(a) \right) \end{aligned}$$

Note that R -module's definition guarantees the commutative of \checkmark (scalar multiplication is direct). ■

Problem III.6.3. Let R be a ring, M an R -module, and $p : M \rightarrow M$ an R -module homomorphism such that $p^2 = p$. Prove that $M \cong \ker p \oplus \operatorname{im} p$.

Proof. We are required to prove that the diagram

$$\begin{array}{ccccc} \ker p & & & & \\ & \searrow i_k & & \nearrow f_k & \\ & & M & \xrightarrow{\exists! \varphi} & N \\ & \nearrow i_m & & \searrow f_m & \\ \operatorname{im} p & & & & \end{array}$$

commutes. Notice that for $x \in \ker p$, $p(x) = 0$, and

$$\text{for } x \in \operatorname{im} p, x - p(x) = p(y) - p(p(y)) = p(y) - p(y) = 0$$

where $p(y) = x$. This suggest that we define φ as

$$\varphi(x) = f_k(x - p(x)) + f_m(p(x))$$

Indeed, if $x \in \ker p$, then $\varphi(x) = f_k(x)$; if $x \in \operatorname{im} p$, then $\varphi(x) = f_m(p(x)) = f_m(x)$ since for $x \in \operatorname{im} p$,

$$p(y) = x, p(p(y)) = p(y) \Rightarrow p(x) = x.$$

But what about $x \in \ker p \cap \operatorname{im} p$? In fact, the only element in the intersection is 0, as such x must have

$$x = p(y) = p(p(y)) = p(x) = 0$$

so φ is well-defined. Now it suffices to check that φ is a homomorphism, which is direct since p, f_k and f_m are both R -homomorphisms, so it preserves the action on M (check yourself if you're not convinced). Therefore by the universal property of coproduct, $\ker p \oplus \operatorname{im} p \cong M$. ■

Problem III.6.4. Let R be a ring, and let $n > 1$. View $R^{\oplus(n-1)}$ as a submodule of $R^{\oplus n}$, via the injective homomorphism $R^{\oplus(n-1)} \hookrightarrow R^{\oplus n}$ defined by

$$(r_1, \dots, r_{n-1}) \hookrightarrow (r_1, \dots, r_{n-1}, 0).$$

Give a one-line proof that

$$\frac{R^{\oplus n}}{R^{\oplus(n-1)}} \cong R.$$

Proof. The surjective map

$$(r_1, \dots, r_{n-1}, r_n) \mapsto r_n.$$

has kernel precisely $R^{\oplus(n-1)}$, therefore by first isomorphism theorem

$$\frac{R^{\oplus n}}{R^{\oplus(n-1)}} \cong R.$$

■

Problem III.6.5. For any ring R and any two sets A_1, A_2 , prove that $(R^{\oplus A_1})^{\oplus A_2} \cong R^{\oplus(A_1 \times A_2)}$.

Proof. By III.6.1, it is equivalent to prove the following diagram commutes:

$$\begin{array}{ccc} (R^{\oplus A_1})^{\oplus A_2} & \xrightarrow{\exists! \varphi} & M \\ j \uparrow & \nearrow f & \\ A_1 \times A_2 & & \end{array}$$

To do this, note that an element in $(R^{\oplus A_1})^{\oplus A_2}$ is a function $g : A_2 \rightarrow R^{\oplus A_1}$, in which we send an element $a_2 \in A_2$ to

$$j_{a_1, a_2}(x) := \begin{cases} 1 & \text{if } x = a_1 \\ 0 & \text{if } x \neq a_1 \end{cases} \quad (\text{p.p.168})$$

this suggests us to define

$$j(a_1, a_2) \mapsto (j_{a_1, a_2}(b_2))(b_1) = \chi_{a_1}(b_1)\chi_{a_2}(b_2)$$

where χ is the indicator function. Then it follows the same pattern as in III.6.1: for $f : A_1 \times A_2 \rightarrow M$ given and any element $\sum_{a_1 \in A_1, a_2 \in A_2} r_{a_1, a_2} (j_{a_1, a_2}(b_2))(b_1) \in (R^{\oplus A_1})^{\oplus A_2}$, define

$$\varphi \left(\sum_{a_1 \in A_1, a_2 \in A_2} r_{a_1, a_2} (j_{a_1, a_2}(b_2))(b_1) \right) = \sum_{a_1 \in A_1, a_2 \in A_2} r_{a_1, a_2} f(a_1, a_2)$$

The commutative of diagram is direct. Finally, the check for φ is a $R - \mathbf{Mod}$ homomorphism is the same as in III.6.1. ■

Problem III.6.7. Let A be any set, and for any module M over a ring R , define

$$M^A := \prod_{a \in A} M, \quad M^{\oplus A} := \bigoplus_{a \in A} M.$$

Prove that $\mathbb{Z}^{\mathbb{N}} \not\cong \mathbb{Z}^{\oplus \mathbb{N}}$.

Proof. Note that $\mathbb{Z}^{\mathbb{N}}$ can be regarded as the collection of functions

$$f : \mathbb{Z} \rightarrow \mathbb{N}$$

which is the collection of all infinite sequences in \mathbb{Z} . This set has uncountably many elements (as one can argue using Cantor's diagonal argument). On the other hand, $\mathbb{Z}^{\oplus \mathbb{N}}$ is also the collection of these function, but with the additional criterion that

$$f(n) = 0 \text{ for all but finitely many } n \in \mathbb{Z}$$

which says that this set collects all finite sequence in \mathbb{Z} , and as we know (i.e. can construct a bijection to \mathbb{Z}), this set is countable. As the cardinality does not match, $\mathbb{Z}^{\mathbb{N}} \not\cong \mathbb{Z}^{\oplus \mathbb{N}}$, as required. ■

Problem III.6.9. Let R be a ring, F a nonzero free R -module, and let $\varphi : M \rightarrow N$ be a homomorphism of R -modules. Prove that φ is onto if and only if for all R -module homomorphisms $\alpha : F \rightarrow N$ there exists an R -module homomorphism $\beta : F \rightarrow M$ such that $\alpha = \varphi \circ \beta$.

Proof. As M is free, it is generated by a set $X = \{x_i\}$ (not necessarily finite).

(\Rightarrow) Let $\{n_i\} \in N$ be such that $\varphi(x_i) = n_i$. If φ is onto, then each n_i corresponds to a $m_i \in M$ such that $\varphi(m_i) = n_i$. We then just define $\beta(x_i) = m_i$, and the commutativity is clear (note that β might not be unique, but that's fine).

(\Leftarrow) If φ is not onto, i.e. there exists $n \in N$ such that $n \notin \text{im } \varphi$, then this also means that $n \notin \text{im}(\varphi \circ \beta)$ for any β . Now we choose a suitable α so $\alpha = \varphi \circ \beta$ does not hold. Indeed, we can define

$$\alpha(x_i) = n$$

for all i . Then the commutativity does not hold for any choice of β , a contradiction. Therefore φ must be surjective. ■

Problem III.6.10. Let M, N , and Z be R -modules, and let $\mu : M \rightarrow Z, \nu : N \rightarrow Z$ be homomorphism of R -modules. Prove that $R\text{-Mod}$ has 'fibered products'(I.5.12).

Proof. As in the case **Set**(I.5.12), we define fibered coproduct by the set of elements that agrees on Z after being pushed by μ and ν :

$$M \times_Z N := \{(m, n) \in M \oplus N : m \in M, n \in N, \mu(m) = \nu(n)\}$$

By the universal property of fibered product on **Set**, the diagram with the choice $\varphi(z) := (f_M(z), f_N(z))$ makes the following diagram

$$\begin{array}{ccccc} P & & & & \\ & \searrow \exists! \varphi & & \searrow f_N & \\ & & M \times_Z N & \xrightarrow{\pi_N} & N \\ & & \downarrow \pi_M & & \downarrow \nu \\ & & M & \xrightarrow{\mu} & Z \end{array}$$

f_M is the curved arrow from P to M .

commutes, regarding in **Set**. Now we check that $M \times_Z N$ indeed is a submodule of $M \oplus N$: for $(m, n) \in M \times_Z N$, $r(m, n) = (rm, rn)$, and since $\mu(m) = \nu(n)$, $r\mu(m) = \mu(rm) = \nu(rn) = r\nu(n)$, so $(rm, rn) \in M \times_Z N$ as required.

Now it remains to check φ is a R -module homomorphism, which is direct. ■

Problem III.6.11. Define a notion of *fibred coproduct* of two R -modules M, N , along an R -module A , in the style of III.6.10 (and cf. I.5.12).

Prove that fibred coproducts exist in $R\text{-Mod}$. The fibred coproduct $M \oplus_A N$ is called the *push-out* of M along ν (or of N along μ).

Proof. The universal property is as the same stated in I.5.12, but by replacing every set with R -modules and every morphism with $R\text{-Mod}$ homomorphisms. We now show that the fibred coproduct is almost the same in Set : define an equivalence relation

$$R = \{(\mu(x), \nu(x)) \in M \oplus N : x \in A\}$$

on $M \oplus N$, and let $M \oplus_A N := (M \oplus N)/R$. We show that R is a submodule, so the quotient make sense. For $(m, n) \in R$,

$$r(m, n) = r(\mu(x), \nu(x)) = (r\mu(x), r\nu(x)) = (\mu(rx), \nu(rx)) \in R$$

which shows that R is indeed an R -module. Now define

$$\varphi((m, n) + R) = f_M(m) + f_N(n)$$

It is a simple check that φ is a R -module homomorphism, and φ is well-defined, using the same argument as in Set (I.5.12). This makes the following diagram

$$\begin{array}{ccccc} A & \xrightarrow{\nu} & N & & \\ \mu \downarrow & & \downarrow i_N & \searrow f_N & \\ M & \xrightarrow{i_M} & M \oplus_A N & \xrightarrow{\exists! \varphi} & Z \\ & \searrow f_M & & & \end{array}$$

commutes, as we check:

- $i_N \nu = i_M \mu$:

$$i_N \nu(x) = (0, \nu(x)) + R = (\mu(x), 0) + R = i_M \mu(x)$$

- $f_M = \varphi i_M$ (resp. $f_N = \varphi i_N$):

$$\varphi i_M(m) = \varphi((m, 0) + R) = f_M(m).$$

■

Problem III.6.14. Prove that the ideal (x_1, x_2, \dots) of the ring $R = \mathbb{Z}[x_1, x_2, \dots]$ is not finitely generated (as an ideal, i.e. as an R -module).

Proof. If it were, then there exists a surjective $R\text{-Mod}$ homomorphism

$$\varphi : R^{\oplus n} \twoheadrightarrow (x_1, x_2, \dots).$$

Then we collect the polynomials

$$\{\varphi(0, \dots, \underset{i\text{-th place}}{1}, \dots, 0)\}_{i=1}^n$$

Since each polynomials can only contain finitely many indeterminates, and there are only finite polynomials, there must be some indeterminates x_j that is not in the domain of φ (as there are countably many indeterminates in the ideal), contradicting to the surjectivity of φ . Therefore (x_1, x_2, \dots) is not finitely generated. ■

Problem III.6.18. Let M be an R -module, and let N be a submodule of M . Prove that if N and M/N are both finitely generated, then M is finitely generated.

Proof. Let $\{a_i + N\}_{i=1}^m$ be generators of M/N , and $\{b_i\}_{i=1}^n$ be generators of N . Then for every $m \in M$, we consider

$$m + N = \sum_{i=1}^m r_i(a_i + N) = \sum_{i=1}^m r_i a_i + N$$

this says that $m - \sum_{i=1}^m r_i a_i \in N$, and therefore we can again write $m - \sum_{i=1}^m r_i a_i = \sum_{j=1}^n s_j b_j$. To this point we showed that every element in M can be generated by $\{a_i, b_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$, showing that M is finitely generated. ■

III.7

Problem III.7.1. Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong 0$.

Proof.

$$0 = \text{im}(0 \longrightarrow M) = \ker(M \longrightarrow 0) = M.$$

Problem III.7.2. Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow M' \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong M'$.

Proof. The map $(M \longrightarrow M')$ is both a monomorphism and an epimorphism by Example III.7.1 and Example III.7.2. By definition, the map is an isomorphism. ■

Problem III.7.3. Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow L \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow N \longrightarrow 0 \longrightarrow \cdots$$

is exact. Show that, up to natural identifications, $L = \ker \varphi$ and $N = \text{coker } \varphi$.

Proof. The map $(L \longrightarrow M)$ is a monomorphism, so by canonical decomposition

$$L = \frac{L}{\ker(L \longrightarrow M)} \cong \text{im}(L \longrightarrow M) = \ker(M \longrightarrow M') = \ker \varphi.$$

The map $(M' \longrightarrow N)$ is an epimorphism, so it follows by first isomorphism theorem that

$$\text{coker } \varphi = \frac{M'}{\text{im } \varphi} = \frac{M'}{\text{im}(M \longrightarrow M')} = \frac{M'}{\ker(M' \longrightarrow N)} \cong N.$$

Problem III.7.6. Prove the 'split epimorphism part of Proposition 7.5, that is, φ has a right-inverse if and only if the sequence

$$0 \longrightarrow \ker \varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0 \text{ splits.}$$

Proof.

(\Leftarrow) If the sequence splits, then by identifying φ with the projection map from $\ker \varphi \oplus N$ to N , we can let $\psi : N \rightarrow \ker \varphi \oplus N$ to be the inclusion, and it gives a right-inverse.

(\Rightarrow) Assume that φ has a right inverse, which says that

$$\begin{array}{ccc} N & \xrightarrow{\psi} & M \\ & \searrow id & \downarrow \varphi \\ & & N \end{array}$$

To prove the statement, we claim that $M \cong \ker \varphi \oplus N$. This isomorphism is given by

$$(k, n) \mapsto k + \psi(n)$$

it has inverse

$$m \mapsto (m - \psi\varphi(m), \varphi(m))$$

Indeed, we check

$$m \mapsto (m - \psi\varphi(m), \varphi(m)) \mapsto m - \psi\varphi(m) + \psi\varphi(m) = m$$

and $m - \psi\varphi(m)$ is in $\ker \varphi$ since

$$\varphi(m - \psi\varphi(m)) = \varphi(m) - \varphi\psi\varphi(m) = 0$$

and the claim is proved. ■

Problem III.7.8. Prove that every exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow 0$$

of R -modules, with F free, splits.

Proof. By exactness, $\varphi : N \rightarrow F$ is surjective. Therefore by III.6.9, for every $\alpha : F \rightarrow F$, there is $\beta : F \rightarrow N$ such that $\alpha = \varphi \circ \beta$. In particular, let $\alpha = id_F$, then $\varphi \circ \beta = id_F$.

$$\begin{array}{ccccccc} & & & & F & & \\ & & & & \downarrow 1 & & \\ & & & \swarrow \beta & & & \\ 0 & \longrightarrow & M & \xrightarrow{i} & N & \xrightarrow{\varphi} & F \longrightarrow 0 \end{array}$$

With this, we now show that $M \oplus F \cong N$. Define

$$h : M \oplus F \rightarrow N, \quad h(m, f) = i(m) + \beta(f)$$

h is clearly an R -module homomorphism, so it remains to show that it is an isomorphism. h is injective: if $h(m, f) = 0$, then

$$i(m) + \beta(f) = 0 \Rightarrow \varphi i(m) + \varphi \beta(f) = 0 \Rightarrow 0 \text{ (definition of chain complex)} + f = 0$$

showing that $f = 0$. Then $i(m) = 0$, so we must have $m = 0$. h is surjective: we want to find m, f such that $i(m) + \beta(f) = n$ for $n \in N$. By applying φ we have

$$\varphi i(m) + \varphi \beta(f) = 0 + f = \varphi(n)$$

so we have the candidate of f . Now it remains to decide m in which $i(m) = n - \beta(\varphi(n))$: notice that by exactness, $\text{im } i = \ker \varphi$, so we check that $\varphi(n - \beta(\varphi(n))) = 0$ to guarantee the existence of m :

$$\varphi(n - \beta(\varphi(n))) = \varphi(n) - \varphi \circ \beta \circ \varphi(n) = \varphi(n) - \varphi(n) = 0$$

Hence h is an isomorphism, and by definition, the sequence splits. ■

Chapter IV

Groups, second encounter

Unless otherwise specified, in the following G denotes a group, e denotes the identity of G . Some description and hints are omitted for simplicity.

Unless otherwise specified, all groups in this chapter are *finite*.

IV.1

Problem IV.1.1. Let p be a prime integer, let G be a p -group, and let S be a set such that $|S| \not\equiv 0 \pmod{p}$. If G acts on S , prove that the action must have fixed points.

Proof. This is direct by Corollary IV.1.3: since $|S| \not\equiv 0 \pmod{p}$, then the set of fixed points Z satisfies $|S| \equiv |Z| \pmod{p}$. ■

Problem IV.1.4. Let G be a group, and let N be a subgroup of $Z(G)$. Prove that N is normal in G .

Proof. For $g \in G$, $n \in N$,

$$gng^{-1} = gg^{-1}n = n \in N.$$

One should note that *normal is not transitive*: if $G \trianglelefteq H$ and $H \trianglelefteq I$, it is in general not true that $G \trianglelefteq I$. ■

Problem IV.1.5. Let G be a group. Prove that $G/Z(G)$ is isomorphic to the group $\text{Inn}(G)$ (II.6.7). Then prove Lemma 1.5 again.

Proof. Let $\varphi : G \rightarrow \text{Inn}(G)$, $\varphi(g) = \gamma_g(a) := gag^{-1}$ be a homomorphism (II.4.8). By construction it is clearly surjective, and the kernel is

$$\ker \varphi = \{g : gag^{-1} = a\} \Rightarrow \{g : ga = ag\} = Z(G)$$

therefore by first isomorphism theorem, $G/Z(G) \cong \text{Inn}(G)$. If $G/Z(G)$ is cyclic, then by II.6.7 G is commutative. ■

Problem IV.1.6. Let p, q be prime integers, and let G be a group of order pq . Prove that either G is commutative or the center of G is trivial. Conclude that every group of order p^2 , for a prime p , is commutative.

Proof. The subgroups can only be of order 1, p , q or pq by Lagrange, and $|Z(G)|$ can be only one of these four. If $|Z(G)| = 1$, then there is nothing to prove; if $|Z(G)| = p$ (or q), then the quotient is cyclic, so it follows by Lemma IV.1.5 that G is commutative; if $|Z(G)| = pq$, then G is clearly commutative.

By Corollary IV.1.9, the center of a nontrivial p -group is nontrivial, so the order of the center for $|G| = p^2$ can not be 1. Then by above, all the remaining cases will conclude that G is commutative. ■

Problem IV.1.8. Let p be a prime number, and let G be a p -group: $|G| = p^r$. Prove that G contains a normal subgroup of order p^k for every nonnegative $k \leq r$.

Proof. We proceed by induction. If $r = 1$ then there is nothing to prove, so we assume that for $n < r$, the p -group with order p^n has a normal subgroup of order p^k for $k \leq n$.

Now consider the center of G : it is abelian and is a nontrivial p -group by Corollary IV.1.9, so by II.8.20, there exists a (normal) subgroup N that is of order p in $Z(G)$. By IV.1.4, N is normal in G , so we can consider the quotient G/N . The quotient is a p -group and has order p^{r-1} , so by induction hypothesis, G/N has normal subgroups of order p^k for $k \leq r-1$, which we name them H_k for each k . By noting that H_k contains N , we can identify each H_k by H_k/N via Proposition II.8.9. Finally, since $|H_k/N| = p^k$, $|H_k| = p^{k+1}$, so we've found normal subgroup of order p^k for $k \leq r$, proving the statement. ■

Problem IV.1.9. Let p be a prime number, G a p -group, and H a nontrivial normal subgroup of G . Prove that $H \cap Z(G) \neq \{e\}$.

Proof. Let G act on itself by conjugation. Since H is normal, it is the union of some conjugacy class and some element of $Z(G)$, with each conjugacy class of order p^n for some n by Corollary II.9.10. If $H \cap Z(G) = \{e\}$, then this means that H only take e from $Z(G)$, and since the order of all conjugacy classes in H are divisible by p , we would arrive at $|H| \equiv 1 \pmod{p}$, a contradiction since $|H|$ must be a multiple of p . ■

Problem IV.1.21. Let H, K be subgroups of a group G , with $H \subseteq N_G(K)$. Verify that the function $\gamma : H \rightarrow \text{Aut}_{\text{Grp}}(K)$ defined by conjugation is a homomorphism of group and that $\ker \gamma = H \cap Z_G(K)$, where $Z_G(K)$ is the centralizer of K .

Proof. Let γ maps h to an automorphism $\varphi_h(k) = hkh^{-1}$. It is a group homomorphism since

$$\gamma(g)\gamma(h) \mapsto \varphi_g\varphi_h(k) = ghkh^{-1}g^{-1} = \varphi(gh) \mapsto \gamma(gh).$$

The kernel of this map is

$$\ker \gamma = \{h \in H : hkh^{-1} = k \ \forall k \in K\} = \{h \in H : hk = kh \ \forall k \in K\} = H \cap Z_G(K).$$

Problem IV.1.22. Let G be a finite group, and let H be a cyclic subgroup of G of order p . Assume that p is the smallest prime dividing the order of G and that H is normal in G . Prove that H is contained in the center of G .

Proof. In the sense of IV.1.21, we have a homomorphism $\gamma : G \rightarrow \text{Aut}_{\text{Grp}}(H)$ since $H \subseteq N_G(H) = G$. By II.4.14, $\text{Aut}_{\text{Grp}}(H)$ has order $\phi(p) = p-1$. But since G does not contain an element of order $p-1$ by the minimality of p , γ can only be the trivial homomorphism, so it has kernel equal to G . But by IV.1.21, $\ker \gamma = G \cap Z_G(H) = Z_G(H)$, so we must have $Z_G(H) = G$, which means that the element that commutes with h are the whole G , i.e. $H \subseteq Z(G)$, as desired. ■

IV.2

Problem IV.2.1. Prove Claim 2.2: Let G be a finite group, let p be a prime divisor of $|G|$, and let N be the number of cyclic subgroups of G of order p . Then $N \equiv 1 \pmod{p}$.

Proof. We proceed with the same argument as in Theorem IV.2.1. Let S be a set that collects the p -tuple

$$(a_1, \dots, a_p)$$

such that $a_1 \cdots a_p = 1$. It is clear that $|S| = |G|^{p-1}$, and since $a_2 \cdots a_p a_1 = 1$, we can consider the action of $\mathbb{Z}/p\mathbb{Z}$ on S , by

$$\alpha_m : (a_1, \dots, a_n) \mapsto (a_{m+1}, \dots, a_p, a_1, \dots, a_m)$$

By Corollary IV.1.3, $|Z| \equiv |S| \pmod{0}$, where Z is the fixed points under $\mathbb{Z}/p\mathbb{Z}$. The fixed points are of form (a, \dots, a) for $a \in G$, and since $(e, \dots, e) \in Z$ and p divides $|Z|$, $|Z| > 1$. Now notice that for each $a \in G$ such that $(a, \dots, a) \in Z$, a is a generator for some cyclic group of order p , so there are $N(p-1) + 1$ (identity) elements in Z . But since $|Z| \equiv 0 \pmod{p}$, we have

$$Np - N + 1 \equiv 0 \pmod{p} \implies N \equiv 1 \pmod{p}$$

as desired. ■

Problem IV.2.2. Let G be a group. A subgroup H of G is *characteristic* if $\varphi(H) \subseteq H$ for every automorphism φ of G .

- Prove that every characteristic subgroups are normal.
- Let $H \subseteq K \subseteq G$, with H characteristic in K and K normal in G . Prove that H is normal in G .
- Let G, K be groups, and assume that G contains a single subgroup H isomorphic to K . Prove that H is normal in G .
- Let K be a normal subgroup of a finite group G , and assume that $|K|$ and $|G/K|$ are relatively prime. Prove that K is characteristic in G .

Proof.

- Consider $\gamma_g(h) := ghg^{-1}$ for all $g \in G$. Then $gHg^{-1} \subseteq H$ by characteristic property of H , so H is normal.
- By normalness of K , we have $gKg^{-1} = K$, so γ_g is an automorphism on K . Then since $\gamma_g(H) \subseteq H$, $gHg^{-1} \subseteq H$, so H is normal.
- Let φ be any automorphism of G . Then $\varphi(H) \cong H \cong K$ since φ is an isomorphism. But since H is the only subgroup that is isomorphic to K , $\varphi(H) = H$, so H is characteristic, hence normal.
- Let φ be any automorphism of G , and let $\pi : G \rightarrow G/K$ be the quotient homomorphism. Let $K' = \varphi(K)$. Then $\pi(K')$ is a subgroup of G/K , so $|\pi(K')|$ divides $|G/K|$. Also, by first isomorphism theorem, $K'/\ker \pi \cong \text{im } \pi = \pi(K')$, so $|\pi(K')|$ divides $|K'| = |K|$. Since $|K|$ and $|G/K|$ are relatively prime, we can only have $|\pi(K')| = 1$, i.e. $\pi(K') = e_{G/H}$. Combining with $\ker \pi = K$, we have

$$\varphi(K) = K' \subseteq \ker \pi = K$$

as desired. ■

Problem IV.2.4. Prove that a nontrivial group G is simple if and only if its only homomorphic image are the trivial group and G itself (up to isomorphism).

Proof.

(\Rightarrow) Let $\varphi : G \rightarrow G'$ be a surjective homomorphism. By first isomorphism theorem, $G/\ker \varphi \cong G'$. But since kernel is a normal subgroup, the only possibility of G' are $G/\{e\} = G$ or $G/G = \{e\}$. (\Leftarrow) If G is not simple, i.e. there are some nontrivial normal subgroup of G , which we call it H , then $\varphi : G \rightarrow G/H, g \mapsto gH$ is a surjective homomorphism, and G/H is neither $\{e\}$ nor G (up to isomorphism), a contradiction. ■

Problem IV.2.5. Let G be a *simple* group, and assume $\varphi : G \rightarrow G'$ is a nontrivial group homomorphism. Prove that φ is injective.

Proof. $\ker \varphi$ can only be $\{0\}$ or G by simpleness. If $\ker \varphi = \{0\}$ then we are done; if $\ker \varphi = G$ then $\varphi = 0$, which can't be by hypothesis. ■

Problem IV.2.6. Prove that there are no simple groups of order 4, 8, 9, 16, 25, 27, 32 or 49. In fact, prove that no p -group of order $\geq p^2$ is simple.

Proof. The center of p -group, by Corollary IV.1.9, is nontrivial. Since center is a normal subgroup, no group of order $p^n, n \geq 2$ is simple. ■

Problem IV.2.9. Let P be a p -Sylow subgroup of a finite group G , and let $H \subseteq G$ be a p -subgroup. Assume $H \subseteq N_G(P)$. Prove that $H \subseteq P$.

Proof. By noting that P is normal in $N_G(P)$ (Remark IV.1.12), we consider PH , which is a subgroup of $N_G(P)$ by Proposition II.8.11. Then by second isomorphism theorem

$$\frac{PH}{P} \cong \frac{H}{P \cap H}$$

Now $|PH| = \frac{|P||H|}{|P \cap H|}$ by II.8.21, and since either $|P \cap H| = 1$ or $|H|$ by Sylow II, PH is a p -group, and it must be P since P is the maximal p -subgroup of G . Then we have $H \subseteq P$ since $PH = P \Leftrightarrow H \subseteq P$. ■

Problem IV.2.10. Let P be a p -Sylow subgroup of a finite group G , and act with P by conjugation on the set of p -Sylow subgroups of G . Show that P is the unique fixed point of this action.

Proof. Let S be the collection of p -Sylow subgroups of G , and let P act on S by conjugation. If H is any p -Sylow that is fixed by P , then we have $H \subseteq N_G(P)$ ($PHP^{-1} = H \Rightarrow HPH^{-1} = P$), so we can apply IV.2.9 and obtain $H \subseteq P$. But by Sylow II, H must be P , proving the statement. ■

This is the end of the solution manual as of February 23, 2020.

Please revisit

<https://github.com/macyayaya/algebra-chapter-0-solutions/releases>

for possible new releases.

Thanks for your reading.