

# Solution to Algebra : Chapter 0 by Paolo Aluffi

macyayaya<sup>1</sup>

Last updated at February 16, 2020

<sup>1</sup><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 If you find this document outside this page, you might have an outdated version of the solution which might have errors, so please be aware.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.
- If you found an error in the solutions, 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
II Groups, first encounter	1
II.1	1
II.2	2
II.3	2
II.4	3
II.5	4
II.6	5
II.7	6
II.8	7
II.9	9
III Rings and modules	11
III.1	11
III.2	12
III.3	13
III.4	14
III.5	14
	15

# 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  $g, h \in G$ ,  $|gh| = |hg|$ .

*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 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  $\gcd(|g|, |h|) = 1$ , 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  $N = |gh|$ . Then one sees that  $(gh)^N = g^N h^N$  since  $g$  and  $h$  commutes. Then

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

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

**Problem II.1.15.** Let  $G$  be commutative 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 and  $r, s$  relatively prime to  $p$  and  $m < n$ . Then by the previous problem we can calculate the order of  $g^{p^m} h^s$ , which is  $p^n r$ . But this element has order bigger than  $|g|$ , contradict 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.*  $1238237^{18238456} \equiv 7^{18238456} = 49^{9119228} = 2401^{4559614} \equiv 1^{4559614} = 1 \pmod{10}$ . ■

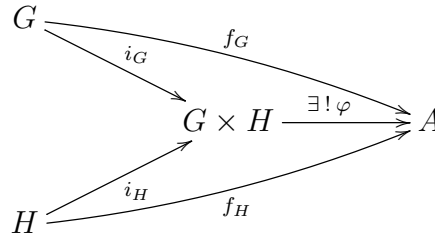
**Problem II.2.17.** Show that if  $m \equiv m' \pmod{n}$ , then  $\gcd(m, n) = 1$  if and only if  $\gcd(m', n) = 1$ .

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

## II.3

**Problem II.3.3.** 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.



To check the universal property, define  $\varphi(g, h) := f_G(g)f_H(h)$ . Now  $\varphi$  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  $\varphi_1$  and  $\varphi_2$  will exhaust all possible element of  $S_3$ , hence force  $\varphi$  to be an isomorphism. But the element  $\varphi(1, 1)$  must be either a 2(or 3)-cycle, and neither  $(1, 1)^2$  nor  $(1, 1)^3$  are  $(0, 0)$ , and  $\varphi$  will map a non-identity element to the identity, a contradiction. ■

## 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.*  $\gamma_g$  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 1.15, all elements have degree that divides  $|g|$ , i.e.  $|h|^{|g|} = 1 \forall h \in G$ . 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  $\varphi$ ,  $\varphi$  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.4.16.** 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  $G = (\mathbb{Z}/p\mathbb{Z})^*$ . 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

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

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:

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

$f$  (curved arrow from  $\mathbb{Z}$  to  $G$ ),  $g$  (curved arrow from  $\{x, y\}$  to  $G$ )

Note that the arrows  $j, g, \varphi$  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  $f = \varphi \circ i$ . 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  $\gamma_g$  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: clearly  $g_e$  is the identity, inverse exists, and the associative clearly holds.

If  $\text{Inn}(G)$  is cyclic, then let  $\gamma_g(a) = gag^{-1}$  be a generator of order  $n$ . Then  $\forall b \in G$  we have  $\gamma_b = \gamma_g^n$ , i.e.  $gbg^{-1} = b^n b b^{-n}$ . This gives  $gb = bg \ \forall b \in G$ , so  $\gamma_g$  is in fact trivial, and hence  $G$  is abelian by II.4.8. 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  $G = \langle a_1, \cdots, a_n \rangle$ , we can represent an element  $g$  uniquely as

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

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

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

as desired.

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

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

To prove, it suffices to "replace" the set  $\{1, \cdots, n\}$  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  $\varphi$  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  $\phi$  be the Euler's  $\phi$ -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 division 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  $\varphi$  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  $\psi$  such that  $\psi \circ \varphi = \text{id}_G$ . Then we would have  $\psi \circ \varphi(a) = \psi \circ \varphi(b)$ , which means  $a = b$ , a contradiction. ■

## II.7

**Problem II.7.7.** 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

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

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  $w = w_1 \cdots w_n$ ,  $\chi$  is the indicator function. The commutative of the coproduct diagram is clear, and  $\phi$  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.8.22.** 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 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  $\mathbf{Grp}$  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.9.13.** 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  $\varphi(xH) = (xgH)g^{-1}$ . 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  $G - \mathbf{Set}(G)$  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  $\psi : \text{Aut}_{G-\mathbf{Set}(G)} \rightarrow G$  by  $\psi(\varphi_g) = g$ . We claim that this is an isomorphism. Indeed, its kernel is precisely  $\varphi_e$ , which is the identity of  $\text{Aut}_{G-\mathbf{Set}(G)}$ . The map is clearly surjective, and it is an homomorphism by construction. Therefore  $\text{Aut}_{G-\mathbf{Set}(G)} \cong G$ . ■

# Chapter III

## Rings and modules

Unless otherwise specified, in the following  $R = (R, +, \cdot)$  denotes an arbitrary ring,  $0, 1$  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.1.6.** 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  $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ , which 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  $i$ . Then let

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

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  $f = a_0$ . 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.2.9.** 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  $a \in C_x$ , then we show that  $a^{-1} \in C_x$ :

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

as desired. ■

**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. ■

### 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.* For any  $x \in R$ ,

$$x\varphi^{-1}(J) = \varphi^{-1}(\varphi(x))\varphi^{-1}(J) = \varphi^{-1}(\varphi(x)J) \subseteq \varphi^{-1}(J)$$

as desired. ■

**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  $R$ .

*Proof.*

( $\Rightarrow$ ) If a nonzero element  $a$  is in the left-ideal  $I$ , then so is  $1_R$  since  $1_R \in a^{-1}I \subseteq I$ . 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 multiplicative inverse, then  $aR$  would be a proper right ideal: It is nonzero, and it does not contain  $1_R$ . Clearly it is an ideal. ■

**Problem III.3.12.** Let  $R$  be commutative. Prove that the set of nilpotent elements forms an ideal of  $R$ .

*Proof.* From III.1.6 we already know that it forms a subgroup of  $(R, +)$ , so it remains to check that it is an ideal. If  $a \in R, r \in I$  and  $r^n = 0$ , then  $ar \in I$  since  $R$  is commutative, so  $(ar)^n = a^n r^n = 0$ .

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

### III.4

**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  $\varphi(i) = j = \varphi(r_1 a_1 + \dots + r_n a_n) = s_1 \varphi(a_1) + \dots + s_n \varphi(a_n)$ , so  $J \subseteq \langle \varphi(a_1), \dots, \varphi(a_n) \rangle$ , and the claim is proved. ■

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

### III.5

**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. Prove that there is a natural bijection between the set of  $R[x]$ -module structures on  $M$  and  $\text{End}_{R\text{-Mod}}(M)$ .

*Proof.* If  $f$  is a  $R$ -endomorphism  $f : M \rightarrow M$ , then we have to show that there are some suitable maps

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

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

$$g(f)(m) = \sum_i a_i f^i(m) \text{ where } f^i = \underbrace{f \circ \dots \circ f}_{i \text{ times}}$$

We can easily check by definition that  $M$  satisfies the property of  $R[x]$ -module, so this gives the injectivity of  $R[x]$ -modules to  $\text{End}_{R\text{-Mod}}(M)$ . To prove surjectivity, if  $M$  is a  $R[x]$ -module, then define  $f(m) = xm$ . Then  $M$  is indeed 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  $\varphi^{-1}$  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. ■

This is the end of the solution as of February 16, 2020.  
Please revisit <https://github.com/macyayaya/algebra-chapter-0-solutions>  
for possible updates.  
Thanks for your reading.