Reading group lecture notes

on Abstract Algebra

Last updated: October 6, 2024

Contents

Remarks

These are lecture notes taken for this Abstract Algebra reading group[1], based on Michael Artin's Algebra [1], and following these free online lecture videos[2]

The notes, problems and solutions are added to the document as the reading group progresses through the course.

The latex code used to produce this document is from a template made by S. Venkatraman:

https://github.com/sara-venkatraman/LaTeX-Templates

[1] https://discord.gg/5bVSwQQR

[2] https://wayback.archive-it.org/3671/20150528171650/https://www.extension.harvard.edu/open-learning-initiative/abstract-algebra

※ Lecture 1

1.1 Groups

Definition 1 (Group)**.** Let G be a set together with a composition law, denoted $\cdot$, following the following properties:

1. For any a, b, c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Associativity of the law)*
2. There exists an identity element 1_G in G such that for any a in G, $a \cdot 1_G = 1_G \cdot a = a$ *(Identity element)*
3. Each element a in G has an inverse b satisfying: $a \cdot b = b \cdot a = 1_G$ *(Inverse element)*

Definition 2 (Order)**.** The ***order*** of a group $(G, \cdot)$, denoted $|G|$, is the number of elements that it contains.

If $|G|$ is finite, G is said to be a ***Finite group***, if not then G is an ***Infinite group***

Example 1.1.

$(\mathbb{Z}, +)$: The set of integers, with addition as its law of composition, – the *additive group of integers.*

$(\mathbb{R}, +)$: The set of real numbers, with addition as its law of composition – the *additive group of real numbers*

$(\mathbb{R}^*, \cdot)$: The set of **nonzero** real numbers with multiplication as its law of composition – the multiplicative group

$(\mathbb{C}, +), (\mathbb{C}^*, \cdot)$: Analogous groups, where $\mathbb{C}$ (resp. $\mathbb{C}^*$), the set of complex numbers (resp. nonzero complex numbers), replaces $\mathbb{R}$ (resp. $\mathbb{R}^\times$).

$(GL_n, \cdot)$: The set of ***Invertible*** $n \times n$ matrices, with the matrix multiplication as its composition law, also named the *general linear group.*

$(Sym(X), \circ)$: The set of all ***bijective*** maps $f : X \longrightarrow X$, together with the *composition of function* as a law, forms a group, usually called the *symmetric group of the set* X.

Remark 1.2.

1. In practice, to refer to a group $(G, \cdot)$, where $\cdot$ is its composition law, we usually just use "G", especially when the set has a "natural" law (e.g. addition for integers, composition of function for sets of functions). When an arbitrary group is discussed, it is also common to refer to the law as "multiplication", this does not mean that the involved set is a set of numbers.
2. The identity element is usually denoted just 1, 1_G, e, or e_G.
3. The inverse of an element a in G is denoted a^{-1}.
4. The inverse of a product is given by $(ab)^{-1} = b^{-1}a^{-1}$. To see why: compute $(ab)(b^{-1}a^{-1})$.

5. If G is a group whose law satisfies $ab = ba$ for any a, b in G, then G is said to be ***Abelian***. The list of examples above contains two non-Abelian groups.

6. We notice that the constraint to take *only* invertible (resp. nonzero) matrices (resp. real numbers) is necessary in order to fulfill property 3 of a group. More generally, in possession of a set S, with an associative law, and an element who does not affect the law[3], it is always possible to form a group, by considering only the subset of S whose elements all have inverses in S (in the sense of 1.3).

Proposition 1 (Cancellation law)**.** let G be a group and a, b, c be elements of G.

- If $ab = ac$ or $ba = ca$, then $b = c$
- If $ab = a$ or $ba = a$, then $b = 1$

Proof. Suppose $ab = ac$, then: $\underbrace{(a^{-1})ab}_{=1b} = \underbrace{(a^{-1})ac}_{=1c}$. □

The other proofs are analogous

1.2 Very brief look into S_n

Consider the symmetric group[4] of the finite set $\{1, 2, \dots, n\}$. This is called the *Permutation group of degree* n and denoted S_n. This forms a group by considering the composition as the group law. If σ and τ are two permutations of $\{1, 2, \dots, n\}$, their respective inverses are their inverse function σ^{-1}, τ^{-1}, and their product is defined as follows:

$$\sigma \cdot \tau = \sigma \circ \tau : j \longmapsto (\sigma \circ \tau)(j) = (\sigma(\tau(j))) \tag{1}$$

Further more, let's introduce the following notation for a given permutation σ:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Precisely, the first line contains all of the elements of the set, and below each element is placed its *image* through σ, giving the second row, which is a *permutation*, AKA a rearrangement of the first line. Since there are $n!$ ways of rearranging the said line, **the order of the group S_n is $n!$**.

BEWARE! n is NOT THE **ORDER of S_n**, it simply refers to the number of integers to permute: $\{1, 2, \dots, n\}$

Example 1.3. There are two possible bijections from $\{1, 2\}$ to itself: the identity map $id : \left(\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right)$, and the map $\sigma : \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$. $\boldsymbol{S_2 = \{id, \sigma\}}$. And the group law is defined by the composition:

$$\sigma \cdot \sigma(1) = \sigma(\sigma(1)) = \sigma(2) = 1$$
$$\sigma \cdot \sigma(2) = \sigma(\sigma(2)) = \sigma(1) = 2$$

so $\sigma^2 = id$.

[3] element e satisfying $ae = ea = a$ for all a in the set
[4] the group of bijections from the set to itself

Example 1.4. Let's analyse the **structure of** S_3 There are $3! = 3 \cdot 2 \cdot 1$ possible permutations of the set $\{1, 2, 3\}$. And those elements are precisely:

$$id = \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \tau_1 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \tau_2 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right), \tau_3 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right), \sigma_1 = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \sigma_2 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)$$

As mentionned before, the group law here is the composition of functions: by using the formula we can compute for example $\sigma_1 \cdot \tau_1$:

$$\sigma_1\tau_1(1) = \sigma_1(\tau_1(1)) = \sigma_1(1) = 2$$
$$\sigma_1\tau_1(2) = \sigma_1(\tau_1(2)) = \sigma_1(3) = 1$$
$$\sigma_1\tau_1(3) = \sigma_1(\tau_1(3)) = \sigma_1(2) = 3$$
$$so\ \sigma_1 \cdot \tau_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \tau_2$$

Using the same method, it is possible to compute

$$\tau_1 \cdot \sigma_1 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \tau_3$$

and we notice that $\tau_1 \cdot \sigma_1 \neq \sigma_1 \cdot \tau_1$ so $\boldsymbol{S_3}$ ***is not abelian***, in fact no permutation group of a set containing more than 3 elements is abelian.

1.3 Subgroups

We noticed that the set GL_n is a set of bijections from R^n to R^n, and so is a subset of $Sym(R^n)$. However, it does NOT follow that *any* subset of a group is also a group, we can convince ourselves of this fact by taking a group G, and considering the subset $G' = G \setminus \{1_G\}$. **The very basic necessity a group needs to have is an identity element:** since every element of G' has an inverse in G, the only candidate as an identity element for G' is the identity element of G, which we've omitted from this set and thus G' does not form a group.

The following criterias encapsulate the constraints required for a subset to form a subgroup:

Definition 3 (Subgroups)**.** let G be a group. A subset H of G is called a *subgroup* of G if it satisfies the following conditions:

1. for any h and k in H, hk is in H. *(H is "closed under the law")*
2. the identity element of G, 1_G is contained in H.
3. for any h in H, its inverse h^{-1} is also contained in H

Remark 1. If H is a subgroup of G, then the closure property implies that if an element a is in H, then for any positive integer n, $a^n = a \cdot \ldots \cdot a$ (n times) is also in G by using induction:

Proof. Let a be an element in a subgroup H of G.

($n = 1$): $a^1 = a$ and a is in H.

Let $k > 1$ and assume a^k is in H. By this induction assumption, a^k is in H, and since a is in H, by closure : $a^k \cdot a = \underbrace{a \cdot \ldots \cdot a}_{ktimes} \cdot a = a^{k+1}$ is also in H. □

Example 1.5.

- For any group G, G is a subgroup itself, and so is the subset $\{1_G\}$, the latter is called *the trivial subgroup*
- The set of *even integers* is a subgroup of the additive integer group: $\mathbb{Z}2 = \{k2|k \in \mathbb{Z}\} \subset \mathbb{Z}$. Note that here the law is addition, the identity element of the group is 0, and the inverse of an element p is $(-p)$. Keeping these in mind, the properties to check are if 0 belongs to the subset, if the inverse $-a$ of an even integer is even, and if the sum $a+b$ of two even integers a and b is even

  (Question: *Is the set of* ***odd*** *integers a* ***subgroup*** *of* $\mathbb{Z}$*?*)
- Given an element a of a group G. The subset $\{a, a^2, a^3, \ldots\}$ is a subgroup of G, named the subgroup *generated* by a, where the powers of a are defined by $a^n = \underbrace{a \cdot \ldots \cdot a}_{n\ times}$ with the convention $a^0 = 1_G$.
- The set of invertible matrices *with determinant 1*: $\{M \in GL_n|det(M) = 1\} \subset GL_n$ is a subgroup of GL_n: it is easy to show that this subset satisfies the properties, by keeping in in mind that $det(AB) = det(A)det(B)$ for any two matrices in GL_n. This subgroup is also denoted SL_n and is called the *Special linear group*
- The set of complex numbers, whose modulus is equal to 1, is a subgroup of the multiplicative group of complex numbers: $\{z \in \mathbb{C}||z| = 1\} \subset \mathbb{C}^*$. Also called *Circle group*, since its elements correspond to the points of the complex plane who lie on the unit circle.

The two last examples are particular cases of a more general way to *find* subgroups of a given group, by using a mapping from a group to another one and adding some additional constraints(here they are $det : GL_n \longrightarrow \mathbb{R}^*$, and $|\cdot| : \mathbb{C}^* \longrightarrow \mathbb{R}^*$). (section 1.6 contains the details).

1.4 $(\mathbb{Z},+)$ and its subgroups

We will keep in mind what has been explained on the additive integer group in the second example from example 1.5.

The following theorem gives a characterization[5] of the subgroups of $\mathbb{Z}$

Theorem 1 (Subgroups of $(\mathbb{Z},+)$)**.** Let S be a subgroup of $(\mathbb{Z},+)$ that is not trivial ($\neq \{0\}$). Then S has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof. Let S be a non-trivial subgroup of $(\mathbb{Z},+)$. By this assumption, S contains an integer n different from 0, and either n or $-n$ (its inverse) is positive. Since S is a subgroup, both n and $-n$ are in S, meaning S necessarily contains a positive integer. Let a be the smallest positive integer in S.

We first show that $\mathbb{Z}a$ is contained in S: Let k be an integer, ka is equal to $\underbrace{a + \ldots + a}_{k terms}$ if $k > 0$, or its inverse: $-(\underbrace{a + \ldots + a}_{|k| terms})$ if $k < 0$. In either case, the sum $(a + \ldots + a)$ is in S[6], and so is its

[5] a precise criteria that is particular to

[6] This is the additive version of remark 1

inverse.

Next we show that S is contained in $\mathbb{Z}a$, in other ways we are going to show that all elements of S is necessarily of the form ka for some integer k. Let n be an integer in S, dividing n by a gives us two integers q and r such that $n = q \cdot a + r$, where $0 \leq r < a$. Since $r = n - q \cdot a$, r is in S, and so r cannot be positive as a is the smallest such integer in S (by choice). Thus $r = 0$ and $n = q \cdot a \in \mathbb{Z}a$ □

1.5 Cyclic groups

Let a be an element of a group G.

Definition 4 (Subgroup generated by an element)**.** The subset $\{a^n | n \in \mathbb{Z}\} = \{1_G, a, a^2, \ldots, a^i, \ldots\}$ is a subgroup of G, it is called the ***subgroup generated by*** a. And is denoted $\langle a \rangle$

Proof. (*that* $\langle a \rangle$ *is a subgroup*) : 1_G is in $\langle a \rangle$, because $a^0 = 1_G$ by convention. For any integers i, j: $a^i \cdot a^j = a^{i+j} \in \langle a \rangle$ so the subset is closed. Finally, the inverse of a^i is given by a^{-i}. □

Remark 1.6. When the law of G is considered as addition, keep in mind that $\langle a \rangle$ is $\{n.a | n \in \mathbb{Z}\} = \{1_G, a, 2a = a + 1, 3a, 4a, \ldots\}$

Definition 5 (Order of an element)**.** Let a be an element of a group G. The ***order of*** a is the order of the group $\langle a \rangle$, and is denoted $\boldsymbol{ord(a)}$, or sometimes $\boldsymbol{o(a)}$.

Proposition 2. Let a be an element of a group G. The following statements are equivalent:

1. $n = ord(a)$ is finite
2. There exists an integer k such that $a^k = 1_G$
3. $\langle a \rangle = \{1_G, a, \ldots, a^n\}$

Moreover, if $ord(a)$ is finite, it is equal to the smallest positive integer satisfying $a^k = 1_G$, and divides any other positive integer satisfying that condition: $\forall j \in \mathbb{N}^*, a^j = 1_G \iff ord(a) \mid j$.

(1) $\implies$ (2) is obvious

(1) $\iff$ (3), seemingly obvious, essentially means that the finiteness of the order of a is equivalent to the elements of $\langle a \rangle$ containing *no other elements* than the n first powers of a. It can be easily proven using $a^k = a^{k \cdot q + r} = (a^k)^q \cdot a^r = 1_G^q \cdot a^r = a^r$ where r is one of $\{0, \ldots, n\}$, whose existence is guaranteed from dividing k by n.

(2) $\implies$ (3) is proven using similar operations as above.

Example 1.7.

- Consider $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$

  By noticing that $\tau^2 = id$, we can deduce that $\langle \tau \rangle$ is finite and has two elements: $\langle \tau \rangle = \{id, \tau\}$. In fact: for an arbitrary integer k: $\tau^{2k+1} = \tau^{2k} \cdot \tau = (\tau^2)^k \cdot \tau = id^k \cdot \tau = \tau$ and $\tau^{2k} = id$, so for an integer n whether it's odd or even, τ^n is in $\{id, \tau\}$. We also conclude that the order of τ is 2.

- The subgroup generated by an element is not necessarily finite, consider for example the matrix $M = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$, whose k-th power is $M^k = \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix}$. For any two distinct integers m and n, $2^m \neq 2^n$, thus there are as many elements in $\langle M \rangle$ as there are integers in $\mathbb{Z}$, which is infinite.
- The subgroup generated by an element can be the whole group: $\mathbb{Z} = \langle 1 \rangle$.

The last example is particular:

Definition 6. Let a be an element of a group G. We say that ***G is generated by a*** if the subgroup generated by a is the whole group: $\boldsymbol{\langle a \rangle = G}$, and ***G is a cyclic group***

1.6 Homomorphisms, Isomorphisms

A few of the most important questions in group theory, is *what groups "are the same"*. Here, similarity between two groups A and B, in some sense, means that if some properties of A are discovered, they also hold for B.

Here is another illustration of what "similarity" means:

Consider the group $S_2 = \{id, \sigma\}$, $\sigma = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)$

Its multiplication table is:

$\circ$	id	σ
id	id	σ
σ	σ	σ^2

Consider the subgroup $\{1, -1\}$ of $\mathbb{C}^\times$. Its multiplication table is:

$\times$	1	-1
1	1	-1
-1	-1	-1^2

Note G_1 the first and G_2 the second group. We notice that both groups look the same, not only because they have equal elements, but also their multiplication tables. The deeper meaning is that it's possible to make a correspondance (a map) from G_1 to G_2 such that two elements a and b from G_1 behave the same way as their two corresponding elements in G_2. (Here id and σ "behave" the same way as "1" and "-1").

Let's formalise:

Definition 7. Let G and H be two groups, with respective laws $*$ and $\cdot$ and $f : G \longrightarrow H$ be a map. We say that ***f is a group homomorphism*** if for any a and b in G, $f(a*b) = f(a) \cdot f(b)$.

It means that, given two elements a and b of G, the two following operations produce the same result:

- operation 1: $(a, b) \xrightarrow{multiply} a * b \xRightarrow{f} f(a * b) = h \in H$

- operation 2: $(a,b) \overset{f}{\Rightarrow} (f(a),f(b)) \xrightarrow{multiply} f(a)\cdot f(b) = h$

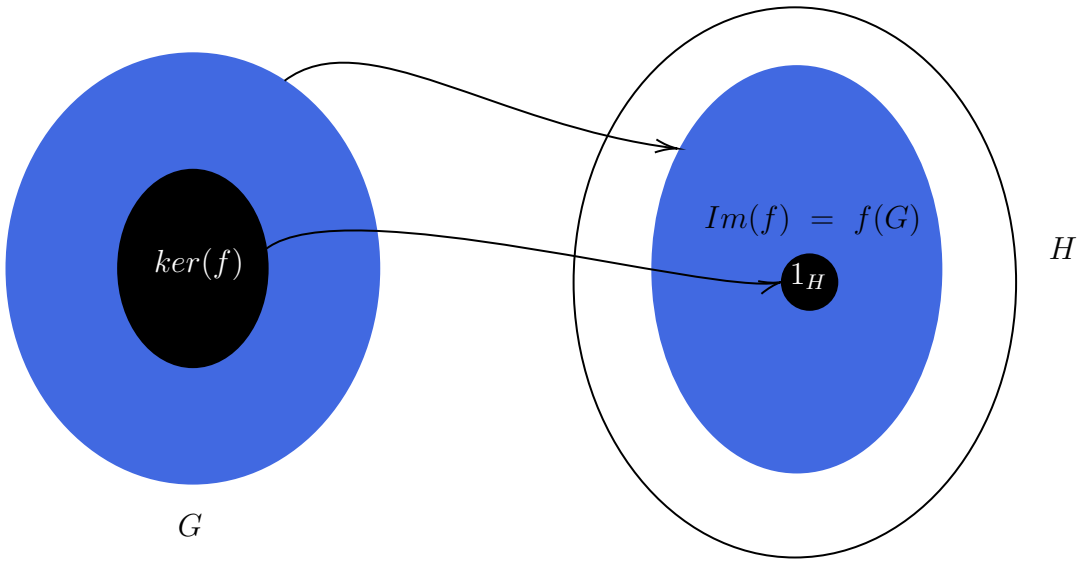
Remark 1.8. Let $f : G \longrightarrow H$ be a group homomorphism. The definition immediately imply the following properties:

- The image of the inverse is the inverse of the image: $f(g^{-1}) = f(g)^{-1}$
- The image of the identity is the identity:$f(1_G) = 1_H$
- The "power" of the image is the image of the power: $f(g^n) = f(g)^n$

Definition 8.

- An ***isomorphism*** is a bijective homomorphism. When there exists an isomorphism between two groups $f : G \longrightarrow H$, G and H are said to be *isomorphic*, and we note: $G \cong H$.
-
- An ***automorphism*** is an isomorphism from a group G to itself: $f : G \longrightarrow G$.

  The set of all automorphisms of a group G is denoted $Aut(G)$
- Let $f : G \longrightarrow H$ be a group homomorphism.
  - The **Kernel** of f is $ker(f) = \{x \in G | f(x) = 1_H\}$: the subset of G whose elements are mapped to 1_H
  - The **Image** of f is $Im(f) = \{f(x) | x \in G\}$: the subset of H who are images of elements of G, also denoted $f(G)$.



Proposition 3. let $f : G \longrightarrow H$ be a group homomorphism, then $ker(f)$ is a subgroup of G and $Im(f)$ is a subgroup of H. (Problem 10)

Proposition. let $f : G \longrightarrow H$ be a group homomorphism, f is injective if and only if $ker(f) = \{1_G\}$.

Proof. Use $f(x) = f(y) \iff f(x)f(y)^{-1} = 1_H \iff f(xy) = 1_H$ □

Here are a few examples of common group homomorphisms:

Example 1.9.

- For any group G, H, we define the *trivial homomorphism* as $f : G \longrightarrow H$, such that $f(x) = 1_H$ for any x in G. Although it has not many interesting properties, its existence means that there is at least one homomorphism between any two arbitrary groups.
- det: $GL_2(\mathbb{R}) \longrightarrow \mathbb{R}^*$ is a group homomorphism whose kernel is $SL_2(\mathbb{R})$, the set of invertible matrices 2×2 with determinant 1. Thus, by proposition 3, *det* is NOT injective, since $SL_2(R)$ does not only contain the identity matrix, but also $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, so *det* is not an isomorphisms. More generally, for $n \geq 2$, $det : GL_n \longrightarrow R^*$ is never injective since there is always a non-identity matrix whose determinant is 1: $\begin{pmatrix} -1 & 0 & & \dots & 0 \\ 0 & -1 & & & 0 \\ & & 1 & & \vdots \\ \vdots & & & \ddots & \\ 0 & \dots & & \dots & 1 \end{pmatrix}$
- exp: $(R, +) \longrightarrow (R\backslash\{0\}, \times)$, defined by $exp(x) = e^x$ is a group homomorphism. This follows from the very well-known algebraic property of exponentiation defined on real numbers: $e^{a+b} = e^a \cdot e^b$
- Let $G = \langle g \rangle$ be a cyclic group. Then $f : \mathbb{Z} \longrightarrow G$ defined by $f(k) = g^k$, is a group homomorphism, and it is an isomorphism if and only if G is infinite. We have previously (see 1.7) used this fact to show that $\left\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle$ is not finite, by considering the isomorphism $k \longmapsto \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix}$ The statements in proposition 2 are used to prove the previous claim.
- Let $G = \langle x \rangle$ and $H = \langle y \rangle$ be two cyclic groups. Under some conditions on $ord(x)$ and $ord(y)$, the map $x^k \longmapsto y^k$ is a group homomorphism. (See Problem 9)
- The absolute value map $|\cdot| : \mathbb{C}^* \longrightarrow \mathbb{R}^*$ is a group homomorphism. It is not an isomorphism as it is neither injective nor surjective.
- Consider the group S_3. We will introduce a new representation of an element σ of S_3 on a 3×3 matrix as follows: for each column i, if $j = \sigma(i)$, place 1 at the j-th row of column i and place 0 everywhere else on that colunm. For example, let $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$, the corresponding matrix is $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. This matrix is invertible, so is in GL_n. Using the analogous process to generalise this process to S_n, We can verify[7] that the map that sends σ to P_σ is an injective group homomorphism from S_n to GL_n.
- Let E be a finite set containing n elements: $\{x_1, \dots, h_n\}$, let $Sym(E)$ be the group of bijections from E to E. Then $Sym(E)$ is isomorphic to S_n. An explicit homomorphism is given by:

$$\begin{aligned} S_n &\longrightarrow Sym(E) \\ \sigma &\longmapsto (f : x_i \mapsto x_{\sigma(i)}) \end{aligned}$$

[7] good exercise

※ Problems and solutions

2.1 Week 1 problems

Problem 1 (2.1.7)**.** let S be any set. Prove that the law of composition defined by $ab = a$ is associative.

Proof. Note that law as $*$. Show that $(a * b) * c = a * (b * c)$: $(a * b) * c = (a) * c = a * c = a = (a) * (X) = (a) * (b * c)$. Where X can be replaced by anything, by definition of the law, so we just replaced it by $(b * c)$ □

Problem 2 (2.2.15)**.**

1. In the definition of subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it is the same as the identity in G. Show that if H has an identity at all, then it is the identity of G, so this definition would be equivalent to the one given.
2. Show the analogous thing for inverses

1. . Let H be a subgroup of G. suppose it has an identity element: 1_H. It is obvious that $1_H \cdot 1_H^{-1} = 1_H$, but $H \subset G$ implies that 1_H is in G, so has an inverse in G: $1_H \cdot 1_H^{-1} = 1_G$, thus $1_G = 1_H$. □
2. let $x \in H$, a its inverse in H and b its inverse in G.

$$ax = 1_H = 1_G = bx$$

The cancellation law immediately implies that $a = b$.

Problem 3 (2.1.5)**.** Assume that the equation $xyz = 1$ holds in a group G. Does it follow that $yzx = 1$? That $yxz = 1$?

$xyz = (xy)z = 1$ means that xy is the inverse of z, by definition of an inverse, their product still gives 1 when commuted.

if $xyz = 1 = yxz$, by cancelling z, we get $xy = yx$, so the second equation holds if and only if the group is abelian.

Problem 4 (2.2.20)**.**

1. Let a, b be elements of an abelian group of orders m, n respectively. What can you say about the order of their product ab?
2. (*) Show by example that the product of elements of finite order in a nonabelian group need not have finite order.

Problem 5 (2.2.1)**.** Determine the elements of the cyclic group generated by the matrix $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

Immediate application of matrix products. It may be helpful to think of Proposition 2

Problem 6 (2.4.6)**.** Let $f : \mathbb{R}^* \longrightarrow \mathbb{C}^\times$ be the map $f(x) = e^{ix}$. Prove that f is a homomorphism and determine its kernel and image.

Proof. Noting that here $\mathbb{R}^*$ refers to the multiplicative group of nonzero real numbers, the fact that f is a homomorphism □

Problem 7 (2.3.11)**.** Prove that the set $Aut(G)$ of automorphisms of a group G forms a group, the law of composition being composition of functions.

Proof. $Aut(G)$ is a group because:

- for any two automorphisms f and g, $f \circ g$ is a morphism: $(f\ circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(g)) = (f \circ g)(a)(f \circ g)(b)$. Moreover the composition of bijective maps is bijective, so $f \circ g$ is an automorphism, The law is well-defined. Moreover: $f \circ g \circ h = f \circ (g \circ h) = (f \circ g) \circ h$, because for an x in G, its image through any of the three maps equals $f(g(h(x)))$. So the law is associative.
- Let id be the identity map on G: $id(x) = x$ for any $x \in G$, it is an automorphism. For any f in $Aut(G)$: $f \circ id : x \longmapsto f(id(x)) = f(x) = id(f(x)) = (id \circ f)(x)$. So $Aut(G)$ contains an identity element: id.
- Let f be in $Aut(G)$. Any bijective map has an inverse, but we need to check that f^{-1} is a group homomorphism: let a, b be two elements of G. note $x = f^{-1}(a), y = f^{-1}(b)$. Then: $ab = f(x)f(y) = f(xy)$, so $xy = f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$

□

Problem 8 (2.3.12)**.** Let G be a group, and let $\varphi : G \longrightarrow G$ be the map $\varphi(x) = x^{-1}$.

1. Prove that φ is bijective.
2. Prove that φ is an automorphism if and only if G is abelian.

φ is bijective because the definition of a group requires each element to have an unique inverse. The second point comes from the remark that $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1}$ which can be $\neq \varphi(a)\varphi(b) = a^{-1}b^{-1}$ unless G is abelian.

Problem 9 (2.4.11)**.** let G, H be cyclic groups, generated by elements x, y. Determine the condition on the orders m, n of x and y so that the map sending $x^i \longmapsto y^i$ is a group homomorphism.

Problem 10 (2.4.3)**.** Prove that the kernel and image of a homomorphism are subgroups.

Proof. Let $f : G \longrightarrow H$ be a group homomorphism. $ker(f)$ is a subgroup of G because:

- $1_G \in ker(f)$
- for any x, y in $ker(f)$: $f(xy) = f(x)f(y) = 1_H 1_H = 1_H$.
- for any x in $ker(f)$: $f(x^{-1}) = f(x)^{-1} = 1_H$.

Note that an element h belonging to $Im(f)$ ensures the existence of g in G such that $f(g) = h$. $Im(f)$ is a subgroup of H because:

- $1_H = f(1_G) \in Im(f)$
- for any $x = f(a), y = f(b) \in im(f)$, $xy = f(a)f(b) = f(ab) \in im(f)$
- for any $x = f(a) \in im(f)$, $x^{-1} = f(a)^{-1} = f(a^{-1}) \in im(f)$

□

Extra problem 1. Let V denote the Klein 4-group. Show that $Aut(V)$ is isomorphic to S_3.

Extra problem 2. Define f: $GL_n(\mathbb{R})$ is the transpose of A. Show that f is an automorphism, but not an inner automorphism for $n \geq 1$.

2.2 Week 2 problems

Problem 11 (2.5.1)**.** Prove that the nonempty fibres of a map form a partition of the domain

Problem 12 (2.5.6)**.**

1. Prove that the relation x conjugate to y in a group G is an equivalence relation on G
2. Describe the elements a whose conjugacy class (=equivalence class) consists of the element a alone.

Problem 13 (2.6.2)**.** Prove directly that distinct cosets do not overlap

Problem 14 (2.6.4)**.** Give an example showing that left cosets and right cosets of $GL_2(\mathbb{R})$ in $GL_2(\mathbb{C})$ are not always equal.

Problem 15 (2.6.5)**.** Let H, K be subgroups of a group G of orders $3, 5$ respectively. Prove that $H \cap K = \{1\}$

References

[1] M. Artin. *Algebra*. Pearson Education, 2011.