Reading group lecture notes

on Abstract Algebra

Last updated: October 5, 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.

[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 and subgroups

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. 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 only one non-Abelian groups.

5. 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

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 : $a^k \cdot a = \underbrace{a \cdot \ldots \cdot a}_{k times} = a^{k+1}$ is also in H. □

Example 1.3.

- 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* $\mathbb{Z}$*?*)

[3] element e satisfying $ae = ea = a$ for all a in the set

- 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 1.4 contains the details).

1.2 $(\mathbb{Z}, +)$ and its subgroups

We will keep in mind what has been explained on the additive integer group in the second example from second example in 1.3.

The following theorem gives a characterization[4] 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[5], and so is its 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 $n = q \cdot a \in \mathbb{Z}a$ □

1.3 Cyclic groups

1.4 Homomorphisms, Isomorphisms

[4] a precise criteria that is particular to
[5] This is the additive version of remark 1

※ 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.

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

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

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 $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$.

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.

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.

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.

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.

References

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