A classical introduction to modern number theory

I'm the author

September 5, 2022

A simple notes template. Inspired by Tufte-LaTeXclass and beautiful notes by

`https://github.com/abrandenberger/course-notes`

1 Groups

1.1 Laws of Composition

Problem 1. Let $a, b \in S$, assume operation of S is associative, and its identity is e. If a is left inverse of b, does this imply that a is right inverse of b?

Proof. Suppose b has left inverse a and right inverse c: $ab = e, bc = e$ but $a \neq c$. Then $ae = a = a(bc) = (ab)c = c$, which is a contradiction. □

1. If $la = e, ar = e$ (it imply that a has both left and right inverse), then $l = r$.
2. If a is invertible, its inverse is unique.
3. Inverse multipy in the opposite order: $(ab)^{-1} = b^{-1}a^{-1}$
4. An element a may have a left inverse or a right inverse, though it is not invertible.

The last statement is unique and interesting.

Lemma 1.1. Every nonzero integer can be written as a product of primes.

Consider how to prove this lemma.

Lemma 1.2. *If $a, b \in \mathbb{Z}$ and $b > 0$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.*

Easy to prove.

Definition 1.1. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis.*

We often see $(a, b) = d$, it means $(a, b) = (d)$ in fact.

Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat.

Definition 1.2. Here's is the beautiful Schrödinger equation

$$i\hbar\frac{\partial}{\partial t}\Psi(x,t) = \left[-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x,t)\right]\Psi(x,t)$$

1.2 *Groups and Subgroups*

A group is a set G together with a law of composition that has the following properties:

1. associative, $(ab)c = a(bc)$ for all $a, b, c \in G$
2. identity element e, $ea = ae = a$ for all $a \in G$
3. for all $a \in G$, a has a inverse b, such that $ab = ba = 1$

An $abeliangroup$ is a group whose law of composition is commutative. For example, the set of nonzero real numbers forms an abelian group under multiplication, and the set of all real numbers forms a abelian group under addition.

Proposition 1.1 (Cancellation Law). *Let a, b, c be elements of a group G whose law of composition is written multiplicatively. If $ab = ac$ or if $ba = ca$, then $b = c$. If $ab = a$ or if $ba = a$, then b=1.*

Proof. Multipy both sides of $ab = ac$ on the left by a^{-1} to obtain $b = c$. The other proofs are analogous. □

1. The $n \times n$ general linear group is the group of all invertible $n \times n$ matrices. It is denoted by $GL_n = n \times n$ invertible matrices A. $GL_n(\mathbb{R}), GL_n(\mathbb{C})$ indicate matrices units are real or complex number. If all matrices of the group have determinant 1, then it's called the special linear group, it's a subgroup of GL_n, it's denoted by SL_n.
2. S_n is the group of permutations of $\{1, 2, \cdots, n\}$, sometimes it's called the symmetric group. The symmetric group S_n is a finite group of order $n!$.

The permutations of a set a, b of two elements are the identity and the transposition. It's a group of order two. Notice the difference between this set and S_2, especially definition of S_n.

Every group G has two obvious subgroups: the group G itself, and the trivial subgroup that consists of the identity element alone.

1.3 *Subgroups of the Additive Group of Integers*

Let a be an integer different from 0. We denote the subset of $\mathbb{Z}$ that consists of all multiples of a by $\mathbb{Z}a$:

$$\mathbb{Z}a = \{n \in Z \mid n = ka \text{ for some k in } \mathbb{Z}\}. \tag{1}$$

Theroem 1.1. Let S be a subgroup of additive group $\mathbb{Z}^+$ (or $(\mathbb{Z}, +)$). Either S is the trivial subgroup 0, or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

$Za \cap Zb = Zm, m = \text{lcm}(a, b)$, and $Za + Zb = Za \cup Zb = Zn, n = \text{gcd}(a, b)$.

1.4 *Cycle Groups*

A group is called cyclic if there exists a $g \in G$ such that $G = \{g^k \mid k \in \mathbb{Z}\}$.

$\langle x \rangle$ is a cyclic subgroup of a group G,

Proposition 1.2. Let x be an element of finite order n in a group, and let k be an integer that is written as $k = nq+r$ where q and r are integers and r is in the range $0 \leq r < n$.

1. $x^k = x^r$.
2. $x^k = 1$ if and only if $r = 0$.
3. Let $d = (k, n)$, the order of x^k is equal to n/d.

Notice the difference between order of x and x^k.

1.5 *Homomorphisms*

Let G and G' be groups, written with multiplicative notation. A **homomorphism** $\phi : G \to G'$ is a map from G to G' such that for all a and b in G

$$\phi(ab) = \phi(a)\phi(b)$$

Intuitively, a homomorhisms is a map that is compatible with the laws of composition in the two groups, and it provides a way to relate different groups, in brief, it's a map from one algebra to another, such as from one group to another.

There are many homomorphism examples, such as the absolute value map $|| : (\mathbb{C}, \times) \to (\mathbb{R}, \times)$, the determinant function det: $GL_n(\mathbb{R}) \to (\mathbb{R}, \times)$.

Proposition 1.3. Let $\phi : G \to G'$ be a group homomorphism.

1. If $a_1, \cdots, c_k \in G$, then $\phi(a_1 \cdots a_k) = \phi(a_1) \cdots \phi(a_k)$.
2. ϕ maps the identity to the identity: $\phi(e_G) = e_G$.
3. ϕ maps the inverse to inverse: $\phi(a^{-1}) = \phi(a)^{-1}$.

Definition 1.3. The image of homomorphism $\rho : G \to H$ is the set $\{\rho(g) \mid g \in G\} \subset H$, written as $\rho(G)$, the kernel of ρ is the set $\{g \mid rho(g) = e_H\}$, written as $\rho(g)^{-1}$.

So $\rho(g)^{-1}$ is the set of all $g \in G$ maped to identity of H. The $\rho(G)$ is a subgroup of H, and $\rho(e_H)^{-1}$ is a subgroup of G. Notice that the kernel of a homomorphism might contain multiple elements. The identity of G must be maped to the identity of H, but not only the identity of G is maped to the identity of H. Such as homomorphism $\rho : \mathbb{Z}_6 \to \mathbb{Z}_3$, $\rho(0, \cdots, 5) = 0, 1, 2, 0, 1, 2$, so image of ρ is $\mathbb{Z}_3$, and kernel of rho is 0,3. Another example is $\rho : \mathbb{Z}_3 \to \mathbb{Z}_6, \rho(n) = 2n$, so the image is $\{0, 2, 4\}$, and again, the kernel is just 0.

left coset: If H is a subgroup of group G, a is in G, then

$$aH = \{ah \mid h \in H\} \tag{2}$$

Proposition 1.4. Let $\phi : G \to G'$ be a homomorphism of groups, and let $a, b \in G$. Let K be the kernel of ϕ. The following four statement are equivalent:

1. $\phi(a) = \phi(b)$
2. $a^{-1}b$ is in K
3. b is in the coset of aK.
4. The coset bK and aK are equal.

Corollary 1.1. A homomorphism $\phi : G \to G'$ is injective if and only if its kernel K is the trivial subgroup {1} of G.

If a and g are elements of a group G, the element gag^{-1} is called the conjugate of a by g.

Definition 1.4. A subgroup N of a group G is a normal subgroup if for every a in N and every g in G, the conjugate gag^{-1} is in N.

Proposition 1.5. The kernel of a homomorphism is a normal subgroup.

Proof. If a is in the kernel of a homomorphism $\phi : G \to G'$ and if any element of G, then $\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)1\phi(g)^{-1} = 1$, therefore gag^{-1} is in the kernel too. So the kernel of a homomorphism is normal. □

The center of a group G, which is often denoted by Z, is the set:

$$Z = \{z \mid zx = zx, z \in G, \text{for all } x \in G\} \tag{3}$$

1.6 *Headings*

Theroem 1.2. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.*

Proof (Theorem 1.1). Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. □

Lemma 1.3. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.*

Proof. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. □

Corollary 1.2. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.*

Proposition 1.6. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris.*

Problem 2. *Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis.*

Proof. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum. $\square$