Notes on "A book of Abstract Algebra", Charles C. Pinter

arnaucube

February 2022

Abstract

Notes on *"A book of Abstract Algebra - by Charles C. Pinter"*, is a *LaTeX* version of handmade notes taken while reading the book. It contains only some definitions and theorems (without proofs), so it is highly recommended to read the actual book instead of the current notes.
This is an unfinished and 'work in progress' document.

Contents

1 Groups **2**

2 Subgroups **2**

3 Functions **3**

4 Isomorphism **3**

5 Cosets **4**

6 Homomorphisms **4**

7 Quotient Groups **5**

8 Rings and Fields **6**

9 Elements of number theory **7**

10 Polynomials **8**

11 Extensions of fields **10**

12 Vector spaces **10**

1 Groups

Def 1.1 (Group)**.** A set G with an operation $*$ which satisfies the axioms:

i. $*$ is *associative*

ii. *(identity element)* there is an element $e \in G$ s.t. $a * e = a$ and $e * a = a$ $\forall a \in G$

iii. *(inverse)* $\forall a \in G$, there is an element $a^{-1} \in G$ s.t. $a{*}a^{-1} = e$ and $a^{-1}{*}a = e$

Def 1.2 (Abelian Group)**.** A group G is said to be *commutative* if $\forall a, b \in G$, $ab = ba$. A commutative group is also called *Abelian*.

Def 1.3 (Order of an element)**.** In a group G, the order of an element $a \in G$ is the least positive integer n such that $a \cdot a \cdots a = a^n = e$. It is represented by $ord(a)$.

Def 1.4 (Order of a group)**.** Order of a group G, is the number of elements in G. It is represented by $|G|$.

Def 1.5 (Cyclic group)**.** Let G be a group, and $a \in G$. If G consists of all the powers of a and nothing else:

$$G = \{a^n : n \in \mathbb{Z}\}$$

then, G is called a *cyclic group*, and a is called its *generator*.
The group G generated by a is defined by $G = \langle a \rangle$.

Thm 1.6. The *order of a cyclic group* is the same as the *order of it's generator*. In other words, for a cyclic group, $|\langle a \rangle| = ord(a)$.

$\langle a \rangle$ defines a cyclic group generated by a. $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$

$|\langle a \rangle|$ defines the order of the cyclic group generated by a.

Thm 1.7. Every subgroup of a cyclic group is cyclic.

2 Subgroups

Def 2.1 (Subgroup)**.** Let G be a group, and H a non-empty subset of G. If

i. the idenity e of G is in H.

ii. H is closed with respect to the operation. Which is for $a, b \in H$, $ab \in H$.

iii. H is closed with respect to inverses. Which is for $a \in H$, $a^{-1} \in H$.

we call H a *subgroup* of G. The operation of H is the same as the operation of G.

Thm 2.2. Every subgroup of a cyclic group is cyclic.

3 Functions

Def 3.1 (Function)**.** If A and B are sets, then a function from A to B is a rule which to every element x in A assigns a unique element y in B.
Functions are represented by $f : A \to B$, where $\forall a \in A \Rightarrow f(a) \in B$.

Def 3.2 (Injective (monomorphism))**.** A function $f : A \to B$ is called *injective* if each element of B is the image of no more than one element of A.

Def 3.3 (Surjective (epimorphism))**.** A function $f : A \to B$ is called *surjective* if each element of B is the image of at least one element of A.
In other words, does not repeat outputs.

Def 3.4 (Bijective (isomorphism))**.** A function $f : A \to B$ is called *bijective* if it is both *injective* and *surjective*.
A function $f : A \to B$ has an inverse iff it is *bijective*. In that case, the inverse f^{-1} is a bijective function from B to A.

In finite sets, if $f : A \to B$ is injective then $|A| \leq |B|$, and if f is surjective then $|B| \leq |A|$. And if f is bijective, then $|A| = |B|$.

Def 3.5 (Composite function)**.** A function $f : A \to B$ and $g : B \to C$ be functions. The *composite function* denoted by $g \circ f$ is a function from A to C defined as follows:

$$[g \circ f](x) = g(f(x)), \forall x \in A$$

Def 3.6 (Permutation)**.** By a *permutation* of a set A we mean a *bijective function from A to A*, that is, a one-to-one correspondence between A and itself.
The set of all the permutations of A, with the operation $\circ$ of composition, is a group.
For any positive integer n, the symmetric group on the set $1, 2, 3, ..., n$ is called the *symmetric group on n elements*, and is denoted by S_n.

4 Isomorphism

Def 4.1 (Isomorphism)**.** Let G_1 and G_2 be groups. A bijective function $f : G_1 \to G_2$ with the property that for any two elements $a, b \in G_1$,

$$f(ab) = f(a)f(b)$$

is called an *isomorphism* from G_1 to G_2.
If there exists an isomorphism from G_1 to G_2, we say that G_1 is *isomorphic* to G_2, symbolized by $G_1 \cong G_2$.

Thm 4.2 (Cayley's Theorem)**.** Every group is isomorphic to a group of permutations.

Thm 4.3. (Isomorphism of cyclic groups)

i. For every positive integer n, every cyclic group of order n is isomorphic to $\mathbb{Z}_n$. Thus, any two cyclic groups of order n are isomorphic to each other.

ii. Every cyclic group of order infinity is isomorphic to $\mathbb{Z}$, and therefore any two cyclic groups of order infinity are isomorphic to each other.

5 Cosets

Def 5.1 (Coset)**.** Let G be a group, and H a subgroup of G. For any element a in G, the symbol aH denotes the set of all products ah, as a remains fixed and h ranges over H. aH is caled a *left coset* of H in G.
In similar fashion, Ha denotes the set of all products ha, as a remains fixed an h ranges over H. Ha is called a *right coset* of H in G.

Thm 5.2. If Ha is any coset of H, there is a one-to-one correspondence from H to Ha (there is a bijection between H and Ha).
If $a \in G$, then $|H| = |Ha|$.

Thm 5.3 (Lagrange's theorem)**.** Let G be a finite group, and H any subgroup of G. The order of G is a multiple of the order of H. $|H|$ divides $|G|$.

Lagrange's theorem can be easily seen by the facts that:

i. cosets partition the group G

ii. $|Ha| = |H|$ (each coset has the same order as H).

By consequence,

Thm 5.4. If G is a group with a prime number p of elements, then G is a cyclic group. Furthermore, any element $a \neq e$ in G is a generator of G.

Thus,

Thm 5.5. The order of any element of a finite group divides the order of the group.

Def 5.6 (Index of H in G)**.** Number of cosets of H in G. Represented by $(G : H)$. Combined with *Lagrange Theorem*, we know that $|G| = |H| \cdot |G : H|$, so,

$$(G : H) = \frac{|G|}{|H|}$$

6 Homomorphisms

Def 6.1 (Homomorhism)**.** If G and G are groups, a *homomorphism* from G to H is a function $f : G \to H$ s.t. for any two elements $a, b \in G$,

$$f(ab) = f(a)f(b)$$

If there exists a homomorphism from G *onto* H, we say that H is a *homomorphic image* of G.

Note: an *isomorphism* is a *bijective homomorphism.*
Example of an *homomorphism*: $f : \mathbb{Z}_6 \to \mathbb{Z}_3$.

Thm 6.2. *Let G and G be groups, and $f : G \to H$ a homomorphism. Then*

i. $f(e) = e$

ii. $f(a^{-1}) = [f(a)]^{-1}, \quad \forall a \in G$

Def 6.3 (Conjugate)**.** A *conjugate* of a is any element of the form xax^{-1}, where $x \in G$.

Def 6.4 (Normal subgroup)**.** Let H be a subgroup of a group G. H is called a *normal* subgroup of G if it is closed with respect to conjugates, that is, if
for any $a \in H$ and $x \in G$, $xax^{-1} \in H$.
Alternatively, we can see that H is a *normal* subgroup iff $\forall a \in G, aH = Ha$.
In an abelian group, every subgroup is normal.

Def 6.5 (Kernel)**.** Let $f : G \to H$ be a homomorphism. The *kernel* of f is the set K of all the elements of G which are carried by f onto the neutral element of H. That is,

$$K = x \in G : f(x) = e$$

Kernel in the context of Extension fields: 11.1

For every homomorphism, the $e \in G$ maps to $e \in H$, so the *kernel* is never empty, it always contains the identity e_G, and if the kernel only contains the identity, then f is one-to-one (injective).

7 Quotient Groups

Quotient group construction is useful as a way of actually manufacturing all the homomorphic images of any group G. Additionally, we can often choose H so as to "factor out" unwanted properties of G, and prserve in G/H only "desirable" traits.

Def 7.1 (Coset multiplication)**.** The coset of a, multiplied by the coset of b, is defined to be the coset of ab. In symbols, $Ha \cdot Hb = H(ab)$.

Thm 7.2. *Let H be a normal subgroup of G. If $Ha = Hc$ and $Hb = Hd$, then $H(ab) = H(cd)$.*

Def 7.3. G/H denotes the set which consists of *all the cosets of H*.
Thus, if $Ha, Hb, Hc, \ldots$ are cosets of H, then $G/H = \{Ha, Hb, Hc, ...\}$.

Thm 7.4 (Quotient group)**.** *G/H with coset multiplication is a group.*

Thm 7.5. *G/H is a homomorphic image of G.*
Conversely, every homomorphic image of G is a quotient group of G.

Thm 7.6. *Let G be a group and H a subgroup of G. Then*

i. $Ha = Hb$ iff $ab^{-1} \in H$

ii. $Ha = H$ iff $a \in H$

8 Rings and Fields

Def 8.1 (Ring)**.** A set A with operations called *addition* and *multiplication* which satisfy the following axioms:

i. A with addition alone is an abelian group.

ii. Multiplication is associative.

iii. Multiplication is distributive over addition. That is, $\forall a, b, c \in A$,

$$a(b+c) = ab + ac$$

$$(b+c)a = ba + ca$$

Def 8.2 (Commutative ring)**.** By definition, addition is commutative in every ring but multiplication is not. When multiplication also is commutative in a ring, we call that ring a *commutative* ring.

Def 8.3 (Unity)**.** A ring does not necessarily have a neutral element for multiplication. If there is in A a neutral element for mulitplication, it is called the *unity* of A, and is denoted by the symbol 1.
If A has a unity, we call A a *ring with unity.*

Def 8.4 (Field)**.** If A is a commutative ring with unity in which every nonzero element is invertible, A is called a *field.*

Thm 8.5 (Finite Field must be over p prime ($\mathbb{F}_p$))**.** Proof from Matan Prasma seminars:
One of the axioms of a field is $\exists$ multiplicative inverse.
If $\mathbb{Z}_n$ with n no prime, then $n = k \cdot l$ for some $1 \leq k,\ l \leq n-1$.
Then in $\mathbb{Z}_n$, $k \cdot l = 0$, but if $k \cdot l = 0$ means that either $k = 0$ or $l = 0$ (otherwise, we could multiply by (eg) k^{-1} and get $k^{-1} \cdot k \cdot l = k^{-1} \cdot 0$, which leads to $1 \cdot l = 0$). which is a contradiction here (since $1 \leq k,\ l \leq n-1$).
Thus $\mathbb{Z}_n$ with n not prime can not be a field.
Conversely, if $n = p$ prime,
for $0 \neq x \in \mathbb{Z}_p$, $gcd(x, p) = 1$, so Extended Euclidean Algorithm gives $u, v \in \mathbb{Z}$ such that $ux + vp = 1$.
Then, $ux = 1 \pmod{p}$, so $u = x^{-1}$, so inverses exist.
Thus $\mathbb{Z}_p$ is a field.

Def 8.6 (Divisor of zero)**.** In any ring, a nonzero element a is called a *divisor of zero* if there is a nonzero element b in the ring such that the product ab or ba is equal to zero.

Def 8.7 (Cancellation property)**.** A ring is said to have the cancellation property if $ab = ac$ or $ba = ca$ implies $b = c$ for any elements a, b, and c in the ring if $a \neq 0$.

Thm 8.8. A ring has the *cancellation property* iff it has no *divisors of zero.*

Def 8.9 (Ideal)**.** A nonempty subset B of a ring A is called an *ideal* of A if B is closed with respect to addition and negatives, and B absorbs products in A. (*Absorbs product*: $\forall b \in B$ and $x \in A$, then $xb, bx \in B$).

Def 8.10 (Principal ideal)**.** A *principal ideal* is an ideal I in a ring R that is generated by a single element $a \in R$ through multiplication by every element of R. In other words $I = aR = \{ar : r \in R\}$.
(eg. Every ideal of $\mathbb{Z}$ is principal).

Def 8.11 (Integral domain)**.** An *integral domain* is defined to be a commutative ring with unity having the cancellation property.

Every field is an integral domain, but the converse is not true (eg. $\mathbb{Z}$ is an integral domain but not a field).

Def 8.12 (Characteristic n)**.** Let A be a ring with unity, the *characteristic* of A is the least positive integer n such that

$$\underbrace{1 + 1 + \cdots + 1}_{n-times} = 0$$

If there is no such positive integer n, A has characteristic 0.

9 Elements of number theory

Def 9.1 (Euclid's lemma)**.** Let m and n be integers, and let p be a prime. If $p|(mn)$, then either $p|m$ or $p|n$.

Thm 9.2 (Factorization into primes)**.** Ever integer $n > 1$ can be expressed as a product of positive primes. That is, there are one or more primes $p_1, \dots, p_r$ such that $n = p_1 p_2 \cdots p_r$.

Thm 9.3 (Unique factorization)**.** Suppose n can be factored into positive primes in two ways, namely,

$$n = p_1 \cdots p_r = q_1 \cdots q_t$$

Then $r = t$, and the p_i are the same numbers as the q_j except, possibly, for the order in which they appear.

From the last two theorems: every integer m can be factored into primes, and the prime factors of m are unique (except for the order).

Thm 9.4 (Little theorem of Fermat)**.** Let p be a prime. Then,

$$a^{p-1} \equiv 1 \pmod{p}, \forall a \not\equiv 0 \pmod{p}$$

So, by taking $a^{p-2} \cdot a \equiv 1 \pmod{p}$, where $a^{p-2} \equiv a^{-1} \pmod{p}$ (the inverse modulo p), we see that $a^p \equiv a \pmod{p}, \forall a \in \mathbb{Z}$, so $a^p - a$ is a multiple of p.

Relation to Lagrange's theorem:
Let $G = \mathbb{Z}_p$, and let H be the multiplicative subgroup of G generated by a (ie. $H = \{1, a, a^2, \ldots\}$). The order of H ($h = |H|$), is also the order of a (ie. smallest $n > 1$ s.t. $a^n = 1 \ mod \ p$).

By Lagrange's theorem, $h \mid |G| = p - 1$, so $p - 1 = h \cdot m$, thus

$$a^{p-1} = (a^h)^m \equiv 1^m \equiv 1 \ mod \ p$$

Another perspective:
We have $a^p \equiv a \pmod{p}$, by dividing by a on both sides, we obtain $a^{p-1} \equiv 1 \pmod{p}$.

Thm 9.5 (Euler's ϕ function)**.** *Euler's ϕ function* describes the number of integers in $\mathbb{Z}/n\mathbb{Z}$ which are relatively prime (coprime) to n.

Thm 9.6 (Euler's theorem)**.** If a and n are relatively prime,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

10 Polynomials

Def 10.1. Let A be a commutative ring with unity, and x an arbitrary symbol. Every expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

is called a *polynomial in x with coefficients in A*, or more simply, a *polynomial in x over A*.

The expressions $a_k x^k$, for $k \in \{1, \ldots, n\}$, are called the *terms* of the polynomial, being $a_n x^n$ the *leading term*, and a_0 the *constant term*. The a_k are called the *coefficients* of x^k, being a_n the *leading coefficient*. And the *degree* of a polynomial $a(x)$ is the greatest n such that the coefficient of x^n is not zero. The polynomial whose leading coefficient is equal to 1 is called *monic*.

Thm 10.2 (Division algorithm for polynomials)**.** If $a(x)$ and $b(x)$ are polynomials over a field F, and $b(x) \neq 0$, there exist polynomials $q(x)$ and $r(x)$ over F such that $a(x) = b(x)q(x) + r(x)$ and $[r(x) = 0$ or $\deg r(x) < \deg b(x)]$.

Thm 10.3. Any two nonzero polynomials $a(x), b(x) \in F[x]$ have a gcd $d(x)$. Furthermore, $d(x)$ can be expressed as a *linear combination*

$$d(x) = r(x)a(x) + s(x)b(x)$$

where $r(x), s(x) \in F[x]$.

Thm 10.4 (Factorization into irreducible polynomials)**.** Every polynomial $a(x)$ of positive degree in $F[x]$ can be written as a product

$$a(x) = kp_1(x)p_2(x)\cdots p_r(x)$$

where k is a constant in F and $p_1(x), \dots, p_r(x)$ are monic irreducible polynomials of $F[x]$.

Thm 10.5 (Unique factorization)**.** If $a(x)$ can be written in two ways as a product of monic irreducibles, say

$$a(x) = kp_1(x)\cdots p_r(x) = lq_1(x)\cdots q_s(x)$$

then $k = l$, $r = s$, and $p_i(x) = q_j(x)$.

Thm 10.6. c is a root of $a(x)$ iff $x - c$ is a factor of $a(x)$.

Thm 10.7. If $a(x)$ has distinct roots $c_1, \dots, c_m$ in F, then $(x-c_1)(x-c_2)\cdots(x-c_m)$ is a factor of $a(x)$.

Thm 10.8. If $a(x)$ has degree n, it has at most n roots.

In finite F, polynomial $\neq$ polynomial function. If F is infinite, polynomial $=$ polynomial function.

For every polynomial with rational coefficients, there is a polynomial with integer coefficients having the same roots. See:

$$a(x) = \frac{k_0}{l_0} + \frac{k_1}{l_1}x + \cdots + \frac{k_n}{l_n}x^n$$

$$= \frac{1}{l_0\cdots l_n} \cdot \underbrace{(k_0 l_1 \cdots l_n + k_1 l_0 l_2 \cdots l_n x + \cdots + k_n l_0 \cdots l_{n-1} x^n)}_{b(x)}$$

$a(x)$ has rational coefficients, $b(x)$ has integer coefficients. $b(x)$ differs from $a(x)$ only by a constant factor ($\frac{1}{l_0\cdots l_n}$), so $a(x)$ and $b(x)$ have the same roots.

$\implies$ $\forall\, p(x) \in \mathbb{Q}[x]$, there is a $f(x) \in \mathbb{R}$ with the same roots (for every polynomial with rational coefficients, there is a polynomial with integer coefficients having the same roots).

Thm 10.9. If s/t is a root of $a(x)$, then $s|a_0$ and $t|a_n$.

Thm 10.10. Suppose $a(x)$ can be factored as $a(x) = b(x)c(x)$, where $b(x), c(x)$ have rational coefficients. Then there are polynomials $B(x), C(x)$ with integer coefficients, which are constant multiples of $b(x)$ and $c(x)$ respectively, such that $a(x) = B(x)C(x)$.

Thm 10.11 (Eisenstein's irreducibility criterion)**.** Let $a(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial with integer coefficients.

If there is a prime p such that $p|a_i$, $\forall i \in \{0, n-1\}$, and $p \not| a_n$ and $p^2 \not| a_0$, then $a(x)$ is irreducible over $\mathbb{Q}$.

11 Extensions of fields

Def 11.1 (Kernel)**.** The *kernel* of σ_c consists of all polynomials $a(x) \in F[x]$ such that c is a root of $a(x)$.

Kernel in the context of Homomorphisms: 6.5

Def 11.2 (Algebraic)**.** $c \in E$ is called *algebraic over F* if it is the root of some nonzero polynomial $a(x) \in F[x]$.

Otherwise, c is called *transcendental over F*.

E/K denotes the (field) extension of E over K.

Thm 11.3 (Basic theorem of field extensions)**.** Let F be a field and $a(x) \in F[x]$ a nonconstant polynomial. There exists an extension field E/F and an element $c \in E$ such that c is a root of $a(x)$.

Let $a(x) \in F[x]$ be a polynomial of degree n. There is an extension field E/F which contains all n roots of $a(x)$.

12 Vector spaces

Def 12.1 (Vector space)**.** A *vector space* over a field F is a set V, with two operations $+, \cdot$, called *vector addition* and *scalar multiplication*, such that

- V with vector addition is an abelian group
- $\forall k \in F$ and $\overrightarrow{a} \in V$, the scalar product $k\overrightarrow{a}$ is an element of V, subject to the following conditions: $\forall k, l \in F,\ \overrightarrow{a}, \overrightarrow{b} \in V$

  i. $k(\overrightarrow{a} + \overrightarrow{b}) = k\overrightarrow{a} + k\overrightarrow{b}$

  ii. $(k + l)\overrightarrow{a} = k\overrightarrow{a} + k\overrightarrow{b}$

  iii. $k(l\overrightarrow{a}) = (kl)\overrightarrow{a}$

  iv. $1\overrightarrow{a} = \overrightarrow{a}$

Def 12.2 (Linear combination)**.** If $\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n} \in V$, and $k_1, k_2, \ldots, k_n$ are scalars, then the vector

$$k_1\overrightarrow{a_1} + k_2\overrightarrow{a_2} + \cdots + k_n\overrightarrow{a_n}$$

is called a *linear combination* of $\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n}$.

The set of all the linear combinations of $\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n}$ is a *subspace of V*.

Def 12.3 (Linear dependancy)**.** Let $S = \{\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n}\}$ be a set of distinct vectors in a vector space V. S is said to be *linearly dependent* if there are scalars $k_1, \ldots, k_n$, not all zero, such that $k_1\overrightarrow{a_1} + k_2\overrightarrow{a_2} + \cdots + k_n\overrightarrow{a_n} = 0$. Which is equivalent to saying that at least one of the vectors in S is a linear combination of the others.

If S is not linearly dependent, then it is *linearly independent.* S is linearly independent iff $k_1\overrightarrow{a_1} + k_2\overrightarrow{a_2} + \cdots + k_n\overrightarrow{a_n} = 0$ implies $k_1 = k_2 = \cdots = k_n = 0$. Which is equivalent to saying thatno vector in S is equal to a linear combination of the other vectors in S.

If $\{\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n}\}$ is linearly dependent, then some a_i is a linear combination of the preceding ones.

If $\{\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n}\}$ spans V, and a_i is a linear combination of the preceding vectors, then $\{\overrightarrow{a_1}, \ldots, \cancel{\overrightarrow{a_i}}, \ldots, \overrightarrow{a_n}\}$ still spans V.

Thm 12.4. Any two bases of a vector space V have the same number of elements.

(This comes from the fact that all bases of $\mathbb{R}^n$ contain exactly n vectors)

If the set $(\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_n})$ spans V, it contains a basis of V.

$\boxed{\text{WIP: covered until chapter 28, work in progress.}}$