Number Theory
MATH3431 UNSW

Jeremy Le

2024T1

Definitions: Purple, Theorems: Blue, Properties/Lemmas: Green

Contents

1 The Ring of Integers

1.1 The Set of All Integers

Divisor Let a and b be integers. We say that a is a divisor of b if there exists an integer k such that $b = ka$. If a is a divisor not equal to b we call it a proper divisor.

Divisibility Properties Let $a, b, c \in \mathbb{Z}$. Then

a) If $a \mid b$ and $b \mid c$ then $a \mid c$.

b) $a \mid a$.

c) If $a \mid b$ and $b \mid a$ then $b = \pm a$.

d) If $a \mid b$ and $a \mid c$ then $a \mid (xb + yc)$ for any $x, y \in \mathbb{Z}$.

Euclid's Theorem There are infinitely many primes in $\mathbb{Z}$.

1.2 Ring

Ring A ring consist of a non-empty set R together with two operations defined on elements of R, addition $(+)$ and multiplication (denoted by juxtaposition, or sometimes by $\star$ or $\times$) where all the following properties hold:

1. Closure under addition: if $a, b \in R$ then $a + b \in R$.
2. Commutativity of addition: for all $a, b \in R, a + b = b + a$.
3. Associativity of addition: for all $a, b, c \in R, (a + b) + c = a + (b + c)$.
4. Zero element: There is an element 0 of R such that if $a \in R$ then $a + 0 = a/$
5. Negatives. $\forall a \in R$ there is $-a \in R$ such that $a + (-a) = 0$.
6. Closure under multiplication: if $a, b \in R$ then $ab \in R$.
7. Associativity of multiplication: $\forall a, b, c \in R, (ab)c = a(bc)$.
8. Distributive laws: for all $a, b, c \in R, a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Subtraction For any a, b in a ring R, we define $a - b = a + (-b)$

Ring Properities Let R be a ring and $a, b, c \in R$. Then the following hold:

1. if $a + b = a + c$ then $b = c$;
2. 0 is unique and $0a = a0 = 0$;
3. for each $a, -a$ is unique;
4. $a - b = 0$ if and only if $a = b$;

5. $-(ab) = (-a)b = a(-b)$;

6. $ab - ac = a(b - c)$ and $ac - bc = (a - b)c$.

Commutative Ring A commutative ring is a ring R in which multiplication is commutative, that is, $ab = ba$ for all $a, b \in R$.

Identity Element An identity element in the ring R is an element, usually denoted by 1, with the propery that $1a = a1 = a$ for all $a \in R$. Sometimes we are more explicit and call 1 the multiplicative identity.

Divisors of Zero In a ring R, if a and b are non-zero elements such that $ab = 0$, then a and b are called divisors of zero.

Integral Domain An integeral domain is a commutative ring with identity in which there are no divisors of zero. Explicilty, an integral domain is a non-empty set R together with operations of addition and multiplcation, such that the ring axioms (1) - (8) hold as well as the following:

9. Commutativity of multiplication. If $a, b \in R$ then $ab = ba$.

10. Identity element. There exists an element 1 of R such that if $a \in R$ then $1a = a$.

11. No divisors of zero. For all $a, b \in R$, if $ab = 0$ then either $a = 0$ or $b = 0$.

Cancellation Law for Integral Domains Let R be an integral domain and $a, b, c \in R$ and suppose $a \neq 0$. If $ab = ac$ then $b = c$.

1.3 Divisibility in Commutative Rings

Divisors in Rings Let α, β be elements in a commutative ring R. We say that α is a divisor of β, denoted by $\alpha \mid \beta$, if there exists an element κ of R usch that $\beta = \kappa\alpha$.

Unit of Rings Let R be a commutative ring with identity. An element of R having a multiplicative increase is called a unit of R.

Associates, Irreducibles and Primes

- Elements a and b of an integral domain R are called associates if $a = ub$, for some unit u of R.

- An element ρ of the integral domain R is said to be irreducible if it has the property

$$\forall \alpha, \beta \in R, \quad \text{if } \rho = \alpha\beta \text{ then } \alpha \text{ or } \beta \text{ is a unit.}$$

- A non-zero, non-unit element ρ of the integral domain R is said to be prime if it has the property

$$\forall \alpha, \beta \in R, \ \text{if} \rho \mid \alpha\beta \text{ then } \rho \mid \alpha \text{ or } \rho \mid \beta.$$

Primes are Irreducible In an integral domain every prime is irreducible.

Greatest Common Divisor Let a, b be integers, not both zero. Then a positive intger g is the greatest common divisor of a and b if and only if g is a common divisor and every common divisor is a factor of g.

GCD in Rings Let a, b be elements in a commutative ring R. An element $g \in R$ is a greatest common divisor of a and b in R if $g \mid a, g \mid b$ and every common divisor of a and b is a factor of g.

1.4 Ideals

Ideal Let R be a commutative ring with identity. A subset I of R is called an ideal of R if it has the following three proprties:

- 0 is in I.
- If a, b are in I then $a + b$ is in I.
- If $a \in I$ and $x \in R$ then $ax \in I$.

Smallest Ideal Let R be a commutative ring with identity, and $\{a_1, \dots, a_n\} \subset R$. Then the set

$$\{r_1 a_1 + \cdots + r_n a_n : r_1, \dots, r_n \in R\}$$

is the smallest ideal of R containing $\{a_1, \dots, a_n\}$.

Principal Ideal An ideal I of a ring R is said to be principal if there exists $a \in R$ such that $I = \langle a \rangle = \{ax : x \in R\}$.

Every Ideal is Principal Every ideal in $\mathbb{Z}$ is principal. In particular, if a, b are not both zero then $\langle a, b \rangle = \langle \gcd(a, b) \rangle$.

Principal Ideal Domain A principal ideal domain is an integral domain in which every ideal is principal.

Integral and Principal Ideal Domains Let R be an integral domain.

a. If R has a division algorithm then R is a principal ideal domain.

b. If R is a principal ideal domain, then every non-zero element of R which is not a unit has a unique (up to associates and order) factorisation into irreducibles.

Big-Oh and Little-Oh Notations For two functions $f(x)$, $f : \mathbb{R} \to \mathbb{C}$, and $g(x)$, $g : \mathbb{R} \to \mathbb{R}^+$, we say that

- $f(x) = O(g(x))$ iff $\limsup_{x \to \infty} |f(x)| / g(x) < \infty$ or, alternatively iff there is a constant $c > 0$ such that $|f(x)| \leq cg(x)$ for all sufficiently large x.

- $f(x) = o(g(x))$ iff $\lim_{x\to\infty} |f(x)|/g(x) = 0$ or, alternatively, iff for any $\epsilon > 0$ we have $|f(x)| \le \epsilon g(x)$ for all sufficiently large x.

Prime Number Theorem (PNT) For $x \to \infty$, we have

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = (1 + o(1))\frac{x}{\log x}.$$

2 Diophantine Equations and Congruences

2.1 Congruences

Cancelling in Congruences Let a, b, c and m be integers, with $c \neq 0$.

a) The congruences $cax \equiv cb \pmod{cm}$ and $ax \equiv b \pmod{m}$ have the same solutions.

b) If $\gcd(c, m) = 1$ then the congruences $cax \equiv cb \pmod{m}$ and $ax \equiv b \pmod{m}$ have the same solutions.

Multiplicative Inverse Let $a \in \mathbb{Z}_m$ and $m \in \mathbb{Z}^+$. If $ax \equiv 1 \pmod{m}$, we call x the multiplicative inverse of a modulo m, or the multiplicative inverse of a in $\mathbb{Z}_m$.

2.2 Arithmetic Functions

Notation of Factors For any positive integer n we define $d(n)$ to be the number of (positive) factors of n, and $\sigma(n)$ to be the sum of all (positive) factors of n.

Formula for $\mathbf{d(n)}$ If $n \in \mathbb{Z}^+$ has canonical factorisation into prime powers $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ then

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_s + 1) = \prod_{k=1}^{s}(\alpha_k + 1)$$

Formula for $\sigma(\mathbf{n})$ If $n \in \mathbb{Z}^+$ has canonical factorisation into prime powers

$$\begin{aligned} n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \text{ then} & \\ \sigma(n) &= (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})\cdots(1 + p_s + p_s^2 + \cdots + p_s^{\alpha_s}) \\ &= \prod_{k=1}^{s} \frac{p_k^{a_k+1} - 1}{p_k - 1} \end{aligned}$$

Multiplicative Functions Suppose that f is a function with domain $\mathbb{Z}^+$. We call f multiplicative if

$$f(mn) = f(m)f(n),$$

whenever $\gcd(m, n) = 1$.

d, σ Multiplicative Both d and σ are multiplicative.

Perfect Numbers A number n is called perfect if $\sigma(n) = 2n$.

Euclid-Euler Let n be even. Then n is perfect if and only if there is an integer $k > 1$ such that $n = 2^{k-1}(2^k - 1)$ and $2^k - 1$ is prime.

3 Introduction to Groups

3.1 Fields

Field A field K is a commutative ring with identity in which every non-zero element has a multiplicative inverse.

No Divisors of Zero in Fields A field contains no divisors of zero.

All fields are Integral Domains A field is an integral domain.

Inverse and GCD An element $n \in \mathbb{Z}_m^*$ has an inverse if and only if $\gcd(m, n) = 1$.

Rings and Fields The ring Z_m is a field if and only if m is prime.

3.2 Units of a Ring

Notation for Set of Units In $\mathbb{Z}_m$, we denote the set of units by $\mathbb{U}_m$.

Units in Commutative Rings with Identity Let R be a commutative ring with identity.

a) 1 is a unit of R

b) If a and b are units in R, then so is their product ab.

c) If a is a unit in R then so is a^{-1}

Units are Closed in Commutative Rings with Identity In any commutative ring with identity, the set of all units is closed under multiplication and inverse.

3.3 Groups

Groups A group is a non-empty set G on which an operation $\star$ is defined, such that the following properties hold:

1. Closure: if $a, b \in G$ then $a \star b \in G$.
2. Associativity: if $a, b, c \in G$ then $(a \star b) \star c = a \star (b \star c)$.

3. Identity element: there is an element e of G such that for all $a \in G$ we have $a \star e = e \star a = a$
4. Inverses: for each a in G there is an element b of G such that $a \star b = b \star a = e$. This element is usually denoted a^{-1}.

Abelian Groups If the operation is commutative, i.e. $a \star b = b \star a$, for all $a, b \in G$, the group is called commutative, or Abelian.

Properties of Groups In any group G the following properties hold.

a There is only one identity element in G.

b Each x in G has only one inverse.

c If $x, y \in G$ then $(xy)^{-1} = y^{-1}x^{-1}$.

d If $x, y, z \in G$ and $xy = xz$ then $y = z$.

3.4 Group Isomorphism

Group Isomorphism Let G and H be groups with operations $\star$ and $\bullet$ rspectively. An isomorphism for G to H is a bijective function $\psi : G \to H$ with the property that

$$\psi(a \star b) = \psi(a) \bullet \psi(b) \quad \text{for all elements } a, b \in G.$$

The groups G and H are said to be isomorphic if there exists such a function.
We write $G \cong H$ to indicate that G and H are isomorphic.

Identities and Inverses in Isomorphic Groups Suppose that G and H are groups with identities e_G and e_H, respectively. Let $\psi : G \to H$ be a group isomorphism. Then

1. $\psi(e_G) = e_H$,
2. $\psi(a^{-1}) = (\psi(a))^{-1}$ for all $a \in G$,
3. $\psi(a^n) = \psi(a)^n$ for all $n \in \mathbb{Z}$,
4. If $\psi : G \to H, \theta : H \to K$ homomorphic then $\theta \circ \psi : G \to K$ is also homomorphic,
5. If $\psi : G \to H$ is a isomorphic then $\psi^{-1} : H \to H$ is also isomorphic.

3.5 Wilson's Theorem

Wilson's Theorem Let $p \geq 2$. Then p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

4 The Structure of $\mathbb{U}_m$ and $\mathbb{Z}_m$

4.1 Subgroups and Cyclic Groups

Subgroup Let G be a group, and let H be a subset of G which is itself a group under the same operations as G. Then we say that H is a subgroup of G.

The Subgroup Lemma Let G be a group and H a non-empty subset of G. Then H is a subgroup of G if and only if it is closed under the group operation and inverse.

Cyclic Groups A group G is said to be cyclic if there exists an element $g \in G$ such that $G = \langle g \rangle$, i.e. G is generated by a single element.

Order of a Group and Element The order of a finite group G is the number of elements in $G, |G|$.
The order of an element g in a group G is the smallest positive integer n (if any) such that $g^n = e$. We write $o(g)$ for the order of the element g.

Distinct Powers of Elements If $g \in G$ has order n, then the elements $e, g, g^2, \ldots, g^{n-1}$ are all distinct.

Isomorphic Cyclic Groups Two finite cyclic groups are isomorphic if and only if they have the same order.

Prime Order is Isomorphic is Cycle Group Any group of prime order p is isomorphic to the cyclic group C_p.

Groups of Prime Order are Abelian Any group of prime order is abelian.

All Subsets Closed under Operation are Subgroups Let G be a group with operation $\star$. If H is a non-empty finite subset of G that is closed under $\star$, then H is a subgroup of G.

Lagrange's Theorem If G is a finite group and H is a subgroup of G, then $|H|$ is a factor of $|G|$.

Left Coset Let G be a group and H a subgroup of G. For any $g \in G$ we define the left coset of H by g to be

$$gH = \{gh \mid h \in H\}.$$

If we used additive notation we would write a coset of H as $g + H$.

Order of Elements in a Group is a Divisor of the Group Suppose G is a group of finite order and $g \in G$. Then $g^{|G|} = e$.

Fermat's Little Theorem If p is a prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary of Fermat's Little Theorem If p is prime and a is any integer, then $a^p \equiv a \pmod{p}$.

Euler's Theorem Let n be a positive integer, and let a be an integer relatively prime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$

4.2 Direct Product of Groups

Cartesian Product Let A and B be two sets. The Cartesian production of the two sets is defined by

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Cartesian Proudct of Any Sets is a Group Let H and K groups with operation $\star$ and $\times$, respectively. The set $H \times K$ with the operation $\bullet$ defined by

$$(h_1, k_1) \bullet (h_2, k_2) = (h_1 \star h_2, k_1 \star k_2)$$

is a group.

Cartesian Product of Groups The group in the above Lemma is called the direct product of H and K and it is denoted by $H \otimes K$.

Condition of I somorphism for Cartesian Products Let G be a finite abelian group. If H and K are subgroups of G such that $|H||K| = |G|$ and $H \cap K = \{e\}$, then the mapping

$$\psi : H \otimes K \to G, \quad \text{where} \quad \psi((h, k)) = h, k$$

is an isomorphism.

Direct Sum The direct sum of two additive abelian subgroups H and K is

$$H \otimes K = \{(h, k) \mid h \in H \text{ and } k \in K\},$$

with operation defined by

$$(h_1, k_1) + (h_2, k_2) = (h_1 + h_2, k_1 + k_2).$$

Decomposition of $\mathbb{Z}_n$ Suppose positive integer n factorises as $n = st$.
If s and t are relatively prime, then $\mathbb{Z}_n \cong \mathbb{Z}_s \oplus \mathbb{Z}_t$.
Conversely, if s and t are not relatively prime, then $\mathbb{Z}_n \not\cong \mathbb{Z}_s \oplus \mathbb{Z}_t$.

Direct Sum Cyclic if Pairwise Relatively Prime Let $s_1, s_2, \ldots, s_k$ be positive integers. Then the direct sum $\mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \cdots \oplus \mathbb{Z}_{s_k}$ is cyclic if and only if $s_1, s_2, \ldots, s_k$ are pairwise relatively prime.

The Chinese Remainder Theorem Suppose that the integers $m_1, m_2, \ldots, m_t$ are pairwise coprime, and let $b_1, b_2, \ldots, b_t$ be any intergers. Then the simulataneous congruences

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \ldots \quad , x \equiv b_t \pmod{m_t}$$

have a unique solution modulo $m_1 m_2 \cdots m_t$.

4.3 Decomposition of $\mathbb{U}_m$

Decomposition of $\mathbb{U}_m$ If $n = st$ is a positive integer, $\mathbb{U}_n \cong \mathbb{U}_s \otimes \mathbb{U}_t$ if and only if s and t are coprime.

Euler Function Multiplicative The Euler's function φ is multiplicative.

Formula for $\varphi(n)$ Let n be a positive integer with canonical factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Then

$$\varphi(n) = \prod_{k=1}^{s} \left(p_k^{a_k} - p_k^{a_k - 1}\right) = \prod_{k=1}^{s} \left(p_k - 1\right) p_k^{a_k - 1} = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$