Arithmetic I Exercises

Boyang Guo

October 22, 2022

Contents

Chapter 1

Rudiments

— —WEEK 1— —

Suppose we have a family of sets $\mathcal{C}$. If for each pair of elements $X, Y \in \mathcal{C}$, we have either $X = Y$ or $X \cap Y = \varnothing$, then we say that $\mathcal{C}$ is a disjoint family of sets or a non-intersecting family of sets. The union of all sets in $\mathcal{C}$ is denoted by

$$\bigsqcup_{X \in \mathcal{C}} X$$

We'll make the assumption that the notation $\bigsqcup$ is only used for a non-intersecting family of sets. That is

$$Y = \bigsqcup_{X \in \mathcal{C}} X$$

if and only if

$$\begin{cases} Y = \bigcup_{X \in \mathcal{C}} X \\ ((\forall X_1, X_2 \in \mathcal{C}), X_1 \cap X_2 \neq \varnothing) \Rightarrow (X_1 = X_2) \end{cases}$$

For any set X, we use the notation 2^X to denote the set of all subsets of X. That is

$$2^X = \{Y | Y \subset X\}$$

1.1

Suppose $f : X \to Y$ is a mapping. Prove that

$$X = \bigsqcup_{y \in Y} f^{-1}(\{y\})$$

1.2

Let $f : X \to Y, g : Y \to X$ be two mappings. Prove that if $gf = \mathrm{id}_X$, then f is injective and g is surjective.

1.3

Use 1.3 to prove that: f is invertible $\Leftrightarrow$ f is bijective.

1.4

Consider the mapping $f : X \to X$ where X is a finite set. Prove that the following six properties are equivalent.

f is injective	f is surjective	f is bijective
f is left-invertible	f is right-invertible	f is invertible

1.5

Suppose $X_1, X_2, \cdots, X_n$ are countable (infinite) sets, prove that their Cartesian product

$$X_1 \times X_2 \times \cdots \times X_n$$

is a countable (infinite) set.

1.6

Suppose $\sim$ is a equivalence relation on X. For every $x \in X$, define a set $[x]$ to be

$$[x] = \{y \in X | x \sim y\} (= \{y \in X | y \sim x\})$$

Prove that

1. Given $x_1, x_2 \in X$, we must have $[x_1] = [x_2]$ or $[x_1] \cap [x_2] = \varnothing$
2. $\bigcup\limits_{x \in X} [x] = X$

(In other words, we have $X = \bigsqcup\limits_{x \in X} [x]$)

We define the **quotient set of X under the relation $\sim$** to be

$$(X/\sim) = \{[x] | x \in X\}$$

Apparently, we have $(X/\sim) \subset 2^X$.

A **partition** $\mathcal{C}$ of a set X is defined to be a subset of 2^X such that every element $W \in \mathcal{C}$ is nonempty and

$$X = \bigsqcup_{W \in \mathcal{C}} W$$

Prove that $(X/\sim)$ is a partition of X.

1.7

Denote the set of all equivalence relations on X by $\mathrm{ER}(X)$. Denote the set of all partitions of X by $\mathrm{Par}(X)$. For any equivalence relation $\sim\in \mathrm{ER}(X)$, we define a partition $\pi_X(\sim) \in \mathrm{Par}(X)$ by

$$\pi_X(\sim) = (X/\sim) = \{[x]|x \in X\}, \text{ where } [x] = \{y \in X|x \sim y\}$$

1. Prove that $\mathrm{ER}(X) \subset 2^{(X^2)}$
2. Prove that $\mathrm{Par}(X) \subset 2^{(2^X)}$
3. Prove that π_X is a bijection

We will denote the inverse of π_X by ρ_X. Prove that if $\mathcal{C} \in \mathrm{Par}(X)$, then $(x_1, x_2) \in \rho_X(\mathcal{C})$ if and only if there exists $W \in \mathcal{C}$ such that $x_1, x_2 \in W$.

Remark.

Sets $\mathrm{ER}(X)$ and $\mathrm{Par}(X)$ have the same cardinality. When $\mathrm{Card}(X) = n$, we have $\mathrm{Card}(\mathrm{ER}(X)) = \mathrm{Card}(\mathrm{Par}(X)) = B_n$, where B_n is the n-th Bell number.

1.8

Suppose $\sim\in \mathrm{ER}(X)$, we define a mapping $p_\sim : X \to \pi_X(\sim)$ by

$$p_\sim(x) = [x]$$

Suppose $f : X \to Y$ is a mapping such that $fx_1 = fx_2$ whenever $x_1 \sim x_2$. Prove that there exists exactly one mapping $f_\sim : \pi_X(\sim) \to Y$ such that

$$f = \left(X \xrightarrow{p_\sim} \pi_X(\sim) \xrightarrow{f_\sim} Y\right)$$

The mapping $f_\sim$ is called the induced mapping of f by $\sim$.

1.9

Suppose $f : X \to Y$ is a mapping, we define a relation $\sim_f$ on X by

$$x_1 \sim_f x_2 \text{ if and only if } fx_1 = fx_2$$

Prove that $\sim_f$ is an equivalence relation on X and

$$\pi_X(\sim_f) = \{f^{-1}(\{y\})|y \in \mathrm{Im} f\}$$

Prove that the induced mapping of f by $\sim_f$ is injective, and it is surjective if and only if f is surjective. Conclude that every mapping is a composition of a projection and an injection.

1.10

In this exercise, we only consider positive integers

1. Prove that $\gcd(n,m)|n, \gcd(n,m)|m$
2. Prove that $n|\text{lcm}(n,m), m|\text{lcm}(n,m)$
3. Suppose $d|n, d|m$, prove that $d|\gcd(n,m)$
4. Suppose $n|D, m|D$, prove that $\text{lcm}(n,m)|D$

1.11

Let $a \in \mathbf{Z}, b \in \mathbf{N}$. Prove that there exists $q, r \in \mathbf{Z}$ where $0 \leq r < b$ such that $a = bq + r$. Show that q, r are **uniquely** determined by a, b.

1.12

Show that if $n, m \in \mathbf{Z}$

$$\{an + bm | a, b \in \mathbf{Z}\} = \gcd(n,m)\mathbf{Z}$$

1.13

Prove that $\{4k+1 | k \in \mathbf{N}\} \cap \mathbf{P}$ and $\{4k-1 | k \in \mathbf{N}\} \cap \mathbf{P}$ are infinite sets.

1.14

The Euler totient function $\varphi : \mathbf{N} \to \mathbf{N}$ is defined by the following:

$$\varphi(n) = \text{Card}(\{m \in \mathbf{N} | 1 \leq m \leq n, \gcd(n,m) = 1\})$$

For example, $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4$. Show that

$$\frac{\varphi(n)}{n} = \prod_{v_p(n) > 0} \left(1 - \frac{1}{p}\right)$$

1.15

Suppose $(X, *)$ is a magma, where for every $a, b \in X$ we have

$$(a * b) * b = a, a * (a * b) = b$$

Prove that $a * b = b * a$ for every $a, b \in X$.

Remark 1

Suppose $r \in \mathbf{Q}$ is a non-zero rational number, then we can write is as $r = \pm\frac{q}{Q}$ where $q, Q \in \mathbf{N}$. The p-adic valuation of r is defined by

$$v_p(r) = v_p(q) - v_p(Q)$$

Notice that this definition is well-defined and is an extension of the original v_p. We define the support set of r to be

$$\mathrm{Supp}(r) = \{p \in \mathbf{P} | v_p(r) \neq 0\}$$

This set is always finite. For example,

$$\mathrm{Supp}\left(\frac{9}{14}\right) = \{2, 3, 7\}$$

Use this notion, we have

$$\frac{\varphi(n)}{n} = \prod_{p \in \mathrm{Supp}(n)} \left(1 - \frac{1}{p}\right)$$

We devide the set Support(r) into two non-intersecting subsets:

$$\mathrm{Supp}^+(r) = \{p \in \mathbf{P} | v_p(r) > 0\}$$
$$\mathrm{Supp}^-(r) = \{p \in \mathbf{P} | v_p(r) < 0\}$$

If $r \in \mathbf{Z}_{\neq 0}$, then $\mathrm{Supp}(r) = \mathrm{Supp}^+(r)$. We define

$$\mathbf{Z}_{(p)} = \{r \in \mathbf{Q} | p \notin \mathrm{Supp}^-(r)\}$$

Remark 2

This may be boring, but if $r \in \mathbf{Q}_{\neq 0}$, then we have

$$|r| = \prod_{p \in \mathrm{Supp}(r)} p^{v_p(r)}$$

Or, equivalently,

$$\ln |r| = \sum_{p \in \mathrm{Supp}(r)} v_p(r) \ln p$$

We define a function $|\cdot|_p : \mathbf{Q} \to \mathbf{R}_{\geq 0}$ by

$$|r|_p = \begin{cases} p^{-v_p(r)}, & r \neq 0 \\ 0, & r = 0 \end{cases}$$

Then we have

- $|r_1 - r_2|_p = 0$ if and only if $r_1 = r_2$
- $|r_1 r_2|_p = |r_1|_p |r_2|_p$
- $|r_1 - r_2|_p + |r_2 - r_3|_p \geq |r_1 - r_3|_p$

1.16

Let m be an odd natural number, prove that

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m} \right)$$

1.17

Suppose we have a system of sets and mappings:

$$A_1 \xleftarrow{\phi_2} A_2 \xleftarrow{\phi_3} A_3 \xleftarrow{\phi_4} A_4 \leftarrow \cdots$$

where every A_n is a non-empty finite set. Prove that we can find a sequence of elements $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n, \ldots$, such that

$$\phi_2 x_2 = x_1, \phi_3 x_3 = x_2, \ldots$$

1.18

Show that 1.17 is wrong if we do not acquire every A_n to be finite.

1.19

Let p be a prime number, and $n \in \mathbf{Z}$ such that $\gcd(p, n) = 1$. Prove that

$$p | (n^{p-1} - 1)$$

1.20

Let p be a prime number, and $0 < n < p$ is an integer. Prove that

$$p | \mathrm{C}_p^n$$

where $\mathrm{C}_p^n = \frac{p!}{n!(p-n)!}$

1.21

Let B_n be the n-th Bell number. Let p be a prime number. Show that

$$p | (B_{n+p} - B_{n+1} - B_n)$$

Chapter 2

Algebraic Structures

— —WEEK 4— —

Groups

2.1

Let $(M, *)$ be a semigroup, if $N \subset M$ is a subset such that for all $a, b \in N$ we have $a * b \in N$, then we say that $N \subset_* M$, or N is a sub-semigroup of M. Prove or disprove:

- If M is a monoid, then N is a monoid
- If M does not have an identity, then N does not have an identity
- If M and N are monoids, then their identities are the same one

2.2

Let M be a monoid (which is by definition a semigroup), and denote the set of all invertible elements of M by $\mathrm{U}(M)$, show that $\mathrm{U}(M)$ is a sub-semigroup of M and itself is even a group. We call it the group of units of M.

2.3

Let Ω be a set, and $M(\Omega) = \{f : \Omega \to \Omega\}$ be the set of mappings, together with the composition operation $\circ$.

- Show that $\mathrm{U}(M(\Omega))$ is the set of all bijective mappings.
- If $\Omega = \{1, 2, \ldots, n\}$, we denote $\mathrm{U}(M(\Omega))$ by S_n. Show that $\mathrm{Card}(\mathrm{S}_n) = n!$

2.4

Let $(G, *)$ be a group (which is by definition a semigroup), and $H \subset_* G$ is a sub-semigroup of G. Show that if

1. the identity $e \in H$
2. for all $h \in H$ we have $h^{-1} \in H$

Then H is not only a semigroup, it is a group.

2.5

Let $(G, *)$ be a group (which is by definition a semigroup), and $H \subset_* G$ is a sub-semigroup of G. Show that if H is a group, then

1. the identity $e \in H$
2. for all $h \in H$ we have $h^{-1} \in H$

2.6

Show that H is a subgroup of G if and only if H is a nonempty subset of G and for all $h_1, h_2 \in H$ we have $h_1^{-1} h_2 \in H$.

2.7

Show that if $\varphi : G_1 \to G_2$ is an isomorphism, then $f(e_1)$ is the identity of G_2, where e_1 is the identity of G_1.

2.8

Show that if $\varphi : G_1 \to G_2$ is an isomorphism, then $f(a^{-1}) = (f(a))^{-1}$.

2.9

Let G be a group, we define a new magma $(G^{\text{op}}, *)$ by $x * y = yx$. Show that $(G^{\text{op}}, *)$ is actually a group, called the opposite group of G.

2.10

Show that G and G^{op} are isomorphic (=find an isomorphism between them).

2.11

Show that if $\varphi : G_1 \to G_2$ is an isomorphism, then the inverse mapping φ^{-1} is an isomorphism. Show that if $\varphi : G \to H$ and $\psi : H \to K$ are isomorphisms, then their composition

$$\psi \circ \varphi : G \to K$$

is an isomorphism.

2.12

An automorphism of a group G is an isomorphism from G to G. Denote the set of all automorphisms of G by $\mathrm{Aut}(G)$. Show that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Perm}(G) = \mathrm{U}(M(G))$. (Hint: Use **2.7**)

2.13

Give an example of two non-isomorphic groups of cardinality 4.

2.14

Write down the Cayley table for S_3 and for $\mathrm{Aut}(\mathrm{S}_3)$. Are these two groups isomorphic?

2.15

Let G be a group, we define $\mathrm{SG}(G)$ to be the sets of all subgroups of G. Suppose $S \subset G$ is a **subset**, we define

$$\langle S \rangle = \bigcap_{S \subset H \in \mathrm{SG}(G)} H$$

1. Prove that $\mathrm{SG}(G)$ is closed under arbitrary intersection.
2. Deduce that $\langle S \rangle \in \mathrm{SG}(G)$, which is called the subgroup generated by S. If $G = \langle S \rangle$, we say that G is generated by S.

2.16

Show that S_4 can be generated by $\{(12), (13), (14)\}$.

Show that S_4 can be generated by $\{(12), \theta\}$, here θ is the mapping $\theta(1) = 2, \theta(2) = 3, \theta(3) = 4, \theta(4) = 1$.

2.17

Find all subgroups of S_4.

2.18

S_n is called the n-th symmetric group. We write down some of its elements:

$$(12) = \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ \vdots \\ n \mapsto n \end{cases}, (13) = \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \\ \vdots \\ n \mapsto n \end{cases}, \ldots, (1n) = \begin{cases} 1 \mapsto n \\ 2 \mapsto 2 \\ 3 \mapsto 3 \\ \vdots \\ n \mapsto 1 \end{cases}, \theta = \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ \vdots \\ n-1 \mapsto n \\ n \mapsto 1 \end{cases}$$

1. Prove that S_n is generated by $\{(12), (13), \ldots, (1n)\}$.
2. Prove that S_n is generated by $\{(12), \theta\}$.
3. Prove the Cayley's theorem: every finite group of cardinality n is isomorphic to some subgroup of S_n.

2.19

Construct a non-abelian group of cardinality 8.

2.20

For $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$, classify all groups of cardinality n.

2.21

Suppose $\varphi : G_1 \to G_2$ is a group homomorphism, show that the image and the kernel of φ

$$\mathrm{im}\varphi = \{\gamma \in G_2 : \exists g \in G_1, \varphi g = \gamma\}$$
$$\ker\varphi = \{g \in G_1 : \varphi g = e\}$$

are subgroups of G_1 and G_2.

2.22

Suppose $\varphi : G_1 \to G_2$ is a group homomorphism, show that φ is injective if and only if $\ker\varphi = 1$, and φ is surjective if and only if $\mathrm{im}\varphi = G_2$.

2.23

Show that if $\varphi : G_1 \to G_2$ is a group homomorphism, then

$$\varphi(x) = \varphi(y) \Leftrightarrow xy^{-1} \in \ker \varphi$$

2.24

The kernel of a group homomorphism is not only a subgroup: it is a **normal** subgroup. To be precise, a subgroup H of G is normal, if and only if for all $h \in H, g \in G$ we have

$$ghg^{-1} \in H$$

Show that the kernel of a group homomorphism $G_1 \to G_2$ is a normal subgroup of G_1.

2.25

Suppose H is a subgroup of G. For any $g \in G$, we define

$$gH = \{gh : h \in H\}$$

Show that $\{gH : g \in G\}$ is a partition of G, and g_1H, g_2H have the same cardinality for any two g_1, g_2.

Conclude that if G is finite, then $\mathrm{Card}(H)$ is a divisor of $\mathrm{Card}(G)$.

2.26

Let G be a group, we define $\mathrm{SG}(G)$ to be the sets of all subgroups of G. Suppose $S \subset G$ is a **subset**, we define

$$\langle S \rangle = \bigcap_{S \subset H \in \mathrm{SG}(G)} H$$

1. Elements of the form $s_1^{\epsilon_1} s_2^{\epsilon_2} \cdot \cdots \cdot s_n^{\epsilon_n}$ where $s_i \in S, \epsilon_i \in \mathbf{Z}$ are called S-words. Prove that every element of $\langle S \rangle$ is a S-word.

2. Suppose $S = \{a\}$ contains one element, we also write $\langle a \rangle$ for $\langle \{a\} \rangle$. This group is automatically a cyclic subgroup of G.

   Suppose $a, b \in G$ with $ab = ba$, and that $\langle a \rangle$ is a finite group of order n, $\langle b \rangle$ is a finite group of order m where $\gcd(n, m) = 1$.

   Prove that $\langle \{a, b\} \rangle$ is a cyclic group of order nm.

3. Consider $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ (as elements of $\mathrm{SL}_2(\mathbf{Z})$ if you want). Prove that these two are elements of finite order, such that ab is an element of infinite order. Also, calculate $\langle \{a, b\} \rangle$.

2.27

1. Prove that every finite group is a subgroup of some bi-generated group (=group that can be generated by only two elements).
2. Recall that there is a group homomorphism $\sigma_G : G \to \mathrm{Aut}(G)$ for every group G, defined by

$$\left(G \xrightarrow{\sigma_G(a)} G \right) = \left(g \mapsto aga^{-1} \right)$$

   Prove that if $G = \mathrm{S}_n$ where $n \neq 2, 6$, then σ_G is an isomorphism.
3. Prove that there is only one epimorphism from S_n to S_2 (where $n \geq 2$).
4. Prove that S_n has only one subgroup, of order $\frac{1}{2}\mathrm{Card}(\mathrm{S}_n)$. This subgroup is called the n-th alternating group, denoted by A_n.

2.28

In this exercise, we study the arithmetics of cyclic groups.

1. Suppose G is a cyclic group, and H is a subgroup of G. Prove that H is also a cyclic group.
2. Suppose G is a cyclic group of infinite order, and H is a non-trivial subgroup of G. Prove that H is also a cyclic group of infinite order.
3. Suppose G is a cyclic group of order n, and H is a subgroup of G. Prove that the order of H divides n.
4. Suppose G is a cyclic group of order n, and m is a natural number dividing n. Prove that G has a unique subgroup of order m.
5. Let G be a cyclic group of order n. An element $g \in G$ is called a generator of G if $G = \langle g \rangle$. Prove that the number of generators of G is $\varphi(n)$.
6. Prove that $\sum_{d|n} \varphi(d) = n$. (Hint: How many elements of C_n, the cyclic group of order n, generates a (cyclic) group of order d?)
7. For any group G, we define

$$\mathbf{u}_d(G) = \{g \in G | g^d = 1\}, u_d(G) = \mathrm{Card}(\mathbf{u}_d(G))$$

   Let G be a cyclic group of order n, and let $d|n$. Prove that $u_d(G) = d$.
8. Prove the following cyclic-forcing theorem:

   Suppose G is finite, and $u_d(G) \leq d$ for all $d \in \mathbf{N}$. Prove that G is cyclic.

— —WEEK 5— —

Rings and Fields

Chapter 3

Ring-theoretic Constructions

Chapter 4

Linear Algebra

Chapter 5

Finite Fields and Reciprocity

Chapter 6

p-adic Numbers

Chapter 7

Hilbert Symbol