

# Contents

<b>1</b>	<b>Groups</b>	<b>4</b>
1.1	Group Theory . . . . .	4
1.1:	Abelian groups of small order . . . . .	5
1.2:	Groups of order 4 . . . . .	5
1.3:	Commutator subgroup . . . . .	6
1.4:	Product of subgroups . . . . .	7
1.5:	Goursat's Lemma . . . . .	7
1.6:	Inner automorphisms . . . . .	8
1.7:	Cyclic automorphism group . . . . .	9
1.8:	Double cosets . . . . .	9
1.2	Normal Subgroups and Indices . . . . .	11
1.9:	Subgroups of finite index . . . . .	11
1.10:	Right and left cosets . . . . .	12
1.3	Group Actions . . . . .	13
1.15:	Fixed point free action . . . . .	13
1.16:	Union of conjugates . . . . .	14
1.19:	Counting fixed points . . . . .	15
1.4	Sylow Theory . . . . .	16
1.20:	Center of p-group . . . . .	17
1.21:	Sylow intersections . . . . .	17
1.22:	Normal subgroup in Sylow . . . . .	18
1.23:	Sylow normalizers . . . . .	18
1.5	Group Structure . . . . .	19
1.24:	Groups of order $p^2$ . . . . .	19
1.25:	Non-abelian groups of order $p^3$ . . . . .	20
1.26:	Groups of order $pq$ . . . . .	21
1.27:	Solvability of small groups . . . . .	22
1.28:	Groups of order $p^2q$ . . . . .	22
1.29:	Groups of order $2pq$ . . . . .	23
1.30:	Sylow in orders 40 and 12 . . . . .	24

1.31: Groups of order $\leq 10$	25
1.6 Permutation Groups	25
1.32: Sylow subgroups of symmetric groups	26
1.33: Sign of a permutation	27
1.34: Dihedral groups	28
1.35: Non-abelian groups of order 8	29
1.36: Conjugacy class of $n$ -cycle	29
1.37: Conjugate cycles	30
1.38: Generating symmetric groups	31
1.7 Alternating Groups	32
1.39: Transitivity of alternating group	33
1.40: Subgroups of index $n$ in $A_n$	33
1.41: Simple group of order 60	34
1.8 Abelian Groups	35
1.42: Torsion group $\mathbb{Q}/\mathbb{Z}$	36
1.43: Subgroup isomorphic to quotient	36
1.44: Index formula	37
1.45: Herbrand quotient	37
1.9 Primitive Groups	39
1.46: Primitive group conditions	39
1.47: Double transitivity	40
1.48: Counting fixed points	42
1.10 Fiber Products and Coproducts	43
1.50: Fiber products in abelian groups	44
1.51: Fiber products in sets	44
1.52: Push-outs in abelian groups	45
1.53: Coproduct of homomorphisms	47
1.54: Tits' coproduct criterion	47
1.55: Fixed points of Möbius transformations	48
1.56: Free subgroup of $GL_2(\mathbb{C})$	49
1.57: Group generated by stabilizers	50
1.11 Problem-Solving Techniques	52
<b>2 Rings</b>	<b>56</b>
2.1 Localization and Prime Ideals	56
2.1: Maximal Ideal in Localization	56
2.2: Surjective Homomorphism Preserves Local Property	57
2.3: Unique Maximal Ideal in Localization	58
2.2 Principal and Factorial Rings	58
2.4: Localization Preserves Principal Property	59
2.5: Localization Preserves Factorial Property	59
2.6: Localization at Prime is Principal	60

2.7: GCD in Principal Rings . . . . .	61
2.3 Group of Units . . . . .	61
2.8: Structure of Units Modulo $p^r$ . . . . .	62
2.4 Quadratic Rings . . . . .	63
2.9: Principal Ring of Gaussian Integers . . . . .	63
2.10: Non-Factorial Quadratic Ring . . . . .	64
2.5 Trigonometric Polynomials . . . . .	65
2.11: Trigonometric Polynomial Ring . . . . .	65
2.6 Dedekind Rings . . . . .	67
2.12: Ring of Arithmetic Functions . . . . .	67
2.13: Finitely Generated Ideals . . . . .	69
2.14: Unique Factorization of Ideals . . . . .	70
2.15: Principal Prime Ideal . . . . .	71
2.16: Localization of Dedekind Ring . . . . .	71
2.17: Divisibility in Dedekind Rings . . . . .	72
2.18: Prime Ideals are Maximal . . . . .	72
2.19: Ideal Class Representatives . . . . .	73
2.7 Problem-Solving Techniques . . . . .	74
<b>3 Modules</b>	<b>76</b>
3.1 Discrete Distributions . . . . .	76
3.1: Discrete Uniform Distribution . . . . .	76
3.2: Acceptance Sampling . . . . .	76
3.3: Bernoulli Trials in Traffic . . . . .	77
3.4: Key Trials . . . . .	77
3.2 Binomial and Poisson Distributions . . . . .	77
3.5: Drug Effectiveness . . . . .	77
3.6: Insect Survival . . . . .	78
3.7: Poisson Chocolate Chips . . . . .	78
3.3 Normal Approximations . . . . .	78
3.8: Theater Competition . . . . .	79
3.4 Exponential Families . . . . .	79
3.28: Exponential Family Verification . . . . .	79
3.5 Inequalities . . . . .	79
3.44: Markov and Chebychev Bounds . . . . .	79
3.46: Chebychev Applications . . . . .	80
3.6 Miscellaneous . . . . .	80
3.25: Hazard Function . . . . .	80
3.26: Hazard Function Verification . . . . .	80

# Chapter 1

## Groups

### 1.1 Group Theory

#### Key Definitions and Theorems:

**Definition:** A *group* is a set  $G$  with a binary operation  $\cdot$  such that:

1. (Associativity)  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  for all  $a, b, c \in G$
2. (Identity) There exists  $e \in G$  such that  $e \cdot a = a \cdot e = a$  for all  $a \in G$
3. (Inverses) For each  $a \in G$ , there exists  $a^{-1} \in G$  such that  $a \cdot a^{-1} = a^{-1} \cdot a = e$

**Definition:** A group is *abelian* if  $a \cdot b = b \cdot a$  for all  $a, b \in G$ .

**Definition:** The *order* of a group  $G$  is the number of elements in  $G$ , denoted  $|G|$  or  $\#(G)$ .

**Definition:** The *order* of an element  $g \in G$  is the smallest positive integer  $n$  such that  $g^n = e$ .

**Lagrange's Theorem:** If  $H$  is a subgroup of a finite group  $G$ , then  $|H|$  divides  $|G|$ .

**Definition:** A *cyclic group* is a group generated by a single element.

**Definition:** A *commutator* in a group  $G$  is an element of the form  $[a, b] = aba^{-1}b^{-1}$ .

**Definition:** The *commutator subgroup*  $G^c$  is the subgroup generated by all commutators.

**Definition:** A subgroup  $H$  of  $G$  is *normal* if  $gHg^{-1} = H$  for all  $g \in G$ .

**Definition:** A *homomorphism* from  $G$  to  $H$  is a function  $\phi : G \rightarrow H$  such that  $\phi(ab) = \phi(a)\phi(b)$ .

**Definition:** An *isomorphism* is a bijective homomorphism.

**Definition:** The *center*  $Z(G)$  of a group  $G$  is the set of elements that commute with every element of  $G$ .

**Definition:** The *normalizer*  $N_G(H)$  of a subgroup  $H$  in  $G$  is the set of elements  $g \in G$  such that  $gHg^{-1} = H$ .

**Product Formula:** If  $H, K$  are subgroups of  $G$  with  $K \subset N_G(H)$ , then  $|HK| = \frac{|H||K|}{|H \cap K|}$ .

### 1.1: Abelian groups of small order

Show that every group of order  $\leq 6$  is abelian.

**Strategy:** Based on Lagrange's theorem and the classification of small groups, systematically check each possible order to determine which groups are abelian. Use the fact that groups of prime order are cyclic and hence abelian.

**Solution:** We prove this by checking each possible order:

**Order 1:** The trivial group is abelian.

**Order 2:** By Lagrange's theorem, any non-identity element has order 2, so the group is cyclic and hence abelian.

**Order 3:** Any non-identity element has order 3, making the group cyclic and abelian.

**Order 4:** There are two groups of order 4: the cyclic group  $\mathbb{Z}_4$  and the Klein four-group  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Both are abelian.

**Order 5:** Any non-identity element has order 5, making the group cyclic and abelian.

**Order 6:** There are two groups of order 6: the cyclic group  $\mathbb{Z}_6$  and the symmetric group  $S_3$ . However,  $S_3$  is not abelian (e.g.,  $(12)(13) \neq (13)(12)$ ), so this statement is actually false. The correct statement should be that every group of order  $\leq 5$  is abelian.

■

### 1.2: Groups of order 4

Show that there are two non-isomorphic groups of order 4, namely the cyclic one, and the product of two cyclic groups of order 2.

**Strategy:** Use Lagrange's theorem to determine possible element orders, then classify groups based on whether they have an element of order 4 or not. Construct explicit isomorphisms to known groups.

**Solution:** Let  $G$  be a group of order 4. By Lagrange's theorem, every element has order 1, 2, or 4.

**Case 1:** If  $G$  has an element of order 4, then  $G$  is cyclic and isomorphic to  $\mathbb{Z}_4$ .

**Case 2:** If every non-identity element has order 2, then  $G$  is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$  (the Klein four-group).

To see this, let  $G = \{e, a, b, c\}$  where  $a^2 = b^2 = c^2 = e$ . Since  $ab \neq a$  and  $ab \neq b$ , we must have  $ab = c$ . Similarly,  $ba = c$ , so  $ab = ba$ . This shows  $G$  is abelian. The map  $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow G$  defined by  $\phi(0, 0) = e$ ,  $\phi(1, 0) = a$ ,  $\phi(0, 1) = b$ ,  $\phi(1, 1) = c$  is an isomorphism.

These are the only two possibilities, and they are non-isomorphic since  $\mathbb{Z}_4$  has an element of order 4 while  $\mathbb{Z}_2 \times \mathbb{Z}_2$  does not. ■

### 1.3: Commutator subgroup

Let  $G$  be a group. A commutator in  $G$  is an element of the form  $aba^{-1}b^{-1}$  with  $a, b \in G$ . Let  $G^c$  be the subgroup generated by the commutators. Then  $G^c$  is called the commutator subgroup. Show that  $G^c$  is normal. Show that any homomorphism of  $G$  into an abelian group factors through  $G/G^c$ .

**Strategy:** To show normality, prove that conjugates of commutators are commutators. For the factorization property, show that any homomorphism to an abelian group sends commutators to the identity, then use the universal property of quotient groups.

**Solution:** First, we show that  $G^c$  is normal. Let  $g \in G$  and  $[a, b] = aba^{-1}b^{-1}$  be a commutator. Then

$$g[a, b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = [gag^{-1}, gbg^{-1}],$$

which is also a commutator. Since  $G^c$  is generated by commutators,  $gG^cg^{-1} \subseteq G^c$  for all  $g \in G$ , so  $G^c$  is normal.

Now let  $\phi : G \rightarrow A$  be a homomorphism into an abelian group  $A$ . For any commutator  $[a, b] = aba^{-1}b^{-1}$ , we have

$$\phi([a, b]) = \phi(aba^{-1}b^{-1}) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = \phi(a)\phi(a)^{-1}\phi(b)\phi(b)^{-1} = 1,$$

since  $A$  is abelian. Therefore,  $\phi$  maps all commutators to the identity, and hence maps  $G^c$  to the identity. This means  $\phi$  factors through  $G/G^c$  via the natural projection  $\pi : G \rightarrow G/G^c$ . ■

#### 1.4: Product of subgroups

Let  $H, K$  be subgroups of a finite group  $G$  with  $K \subset N_H$ . Show that

$$\#(HK) = \frac{\#(H)\#(K)}{\#(H \cap K)}.$$

**Strategy:** Use the counting principle by defining a surjective map from  $H \times K$  to  $HK$  and counting the number of preimages of each element. The condition  $K \subset N_H$  ensures that  $HK$  is a subgroup.

**Solution:** Since  $K \subset N_H$ , we have  $HK = KH$  and  $HK$  is a subgroup of  $G$ . Consider the map  $\phi : H \times K \rightarrow HK$  defined by  $\phi(h, k) = hk$ .

For any  $x \in HK$ , we can write  $x = hk$  for some  $h \in H$  and  $k \in K$ . The number of preimages of  $x$  under  $\phi$  is the number of pairs  $(h', k')$  such that  $h'k' = hk$ .

If  $h'k' = hk$ , then  $h^{-1}h' = kk'^{-1} \in H \cap K$ . Let  $t = h^{-1}h' = kk'^{-1} \in H \cap K$ . Then  $h' = ht$  and  $k' = tk$ . Conversely, for any  $t \in H \cap K$ , the pair  $(ht, tk)$  maps to  $hkt = hk$  since  $t \in K \subset N_H$ .

Therefore, each element of  $HK$  has exactly  $\#(H \cap K)$  preimages under  $\phi$ . By the counting principle,

$$\#(H) \cdot \#(K) = \#(H \times K) = \#(HK) \cdot \#(H \cap K),$$

which gives the desired formula. ■

#### 1.5: Goursat's Lemma

Let  $G, G'$  be groups, and let  $H$  be a subgroup of  $G \times G'$  such that the two projections  $p_1 : H \rightarrow G$  and  $p_2 : H \rightarrow G'$  are surjective. Let  $N$  be the kernel of  $p_2$  and  $N'$  be the kernel of  $p_1$ . One can identify  $N$  as

a normal subgroup of  $G$ , and  $N'$  as a normal subgroup of  $G'$ . Show that the image of  $H$  in  $G/N \times G'/N'$  is the graph of an isomorphism

$$G/N \approx G'/N'.$$

**Strategy:** Use the first isomorphism theorem to show that the natural map from  $H$  to  $G/N \times G'/N'$  is bijective, then prove that this bijection is the graph of a homomorphism by showing it preserves the group structure.

**Solution:** First, note that  $N = \{(g, 1) \in H : g \in G\}$  and  $N' = \{(1, g') \in H : g' \in G'\}$ . Since  $p_1$  and  $p_2$  are surjective,  $N$  and  $N'$  are normal subgroups of  $G$  and  $G'$  respectively.

Consider the map  $\phi : H \rightarrow G/N \times G'/N'$  defined by  $\phi(h) = (p_1(h)N, p_2(h)N')$ . The kernel of  $\phi$  is  $N \cap N' = \{(1, 1)\}$ , so  $\phi$  is injective.

For any  $(gN, g'N') \in G/N \times G'/N'$ , since  $p_1$  and  $p_2$  are surjective, there exists  $h \in H$  such that  $p_1(h) = g$  and  $p_2(h) = g'$ . Then  $\phi(h) = (gN, g'N')$ , so  $\phi$  is surjective.

The image of  $H$  under  $\phi$  is the graph of a function  $f : G/N \rightarrow G'/N'$  defined by  $f(gN) = g'N'$  where  $(g, g') \in H$ . This function is well-defined because if  $(g_1, g'_1), (g_2, g'_2) \in H$  with  $g_1N = g_2N$ , then  $(g_1^{-1}g_2, g_1'^{-1}g_2') \in N$ , so  $g_1'^{-1}g_2' \in N'$ , which means  $g_1'N' = g_2'N'$ .

The function  $f$  is a homomorphism because if  $(g_1, g'_1), (g_2, g'_2) \in H$ , then  $(g_1g_2, g'_1g'_2) \in H$ , so  $f(g_1g_2N) = g'_1g'_2N' = f(g_1N)f(g_2N)$ .

Finally,  $f$  is bijective because  $\phi$  is bijective, so  $f$  is an isomorphism. ■

## 1.6: Inner automorphisms

Prove that the group of inner automorphisms of a group  $G$  is normal in  $\text{Aut}(G)$ .

**Strategy:** Show that conjugating an inner automorphism by any automorphism gives another inner automorphism. Use the fact that conjugation by  $\phi$  sends the inner automorphism  $\psi_g$  to  $\psi_{\phi(g)}$ .

**Solution:** Let  $\text{Inn}(G)$  be the group of inner automorphisms of  $G$ . We need to show that for any  $\phi \in \text{Aut}(G)$  and any inner automorphism  $\psi_g$  (conjugation by  $g \in G$ ), we have  $\phi \circ \psi_g \circ \phi^{-1} \in \text{Inn}(G)$ .



For any  $x \in G$ ,

$$(\phi \circ \psi_g \circ \phi^{-1})(x) = \phi(\psi_g(\phi^{-1}(x))) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)x\phi(g)^{-1} = \psi_{\phi(g)}(x).$$

Therefore,  $\phi \circ \psi_g \circ \phi^{-1} = \psi_{\phi(g)}$ , which is an inner automorphism. This shows that  $\text{Inn}(G)$  is normal in  $\text{Aut}(G)$ . ■

### 1.7: Cyclic automorphism group

Let  $G$  be a group such that  $\text{Aut}(G)$  is cyclic. Prove that  $G$  is abelian.

**Strategy:** Use the fact that  $\text{Inn}(G)$  is a subgroup of the cyclic group  $\text{Aut}(G)$ , so it's also cyclic. Then show that if  $G/Z(G)$  is cyclic, then  $G$  is abelian by expressing every element in terms of a generator and central elements.

**Solution:** Since  $\text{Inn}(G)$  is a subgroup of  $\text{Aut}(G)$  and  $\text{Aut}(G)$  is cyclic,  $\text{Inn}(G)$  is also cyclic.

The map  $\phi : G \rightarrow \text{Inn}(G)$  defined by  $\phi(g) = \psi_g$  (conjugation by  $g$ ) is a homomorphism with kernel  $Z(G)$ , the center of  $G$ . Therefore,  $G/Z(G) \cong \text{Inn}(G)$  is cyclic.

Let  $gZ(G)$  be a generator of  $G/Z(G)$ . Then every element of  $G$  can be written as  $g^n z$  for some  $n \in \mathbb{Z}$  and  $z \in Z(G)$ . For any two elements  $g^n z_1$  and  $g^m z_2$ ,

$$(g^n z_1)(g^m z_2) = g^{n+m} z_1 z_2 = g^{m+n} z_2 z_1 = (g^m z_2)(g^n z_1),$$

since  $z_1, z_2 \in Z(G)$  commute with everything. This shows that  $G$  is abelian. ■

### 1.8: Double cosets

Let  $G$  be a group and let  $H, H'$  be subgroups. By a double coset of  $H, H'$  one means a subset of  $G$  of the form  $HxH'$ .

(a) Show that  $G$  is a disjoint union of double cosets.

- (b) Let  $\{c\}$  be a family of representatives for the double cosets. For each  $a \in G$  denote by  $[a]H'$  the conjugate  $aH'a^{-1}$  of  $H'$ . For each  $c$  we have a decomposition into ordinary cosets

$$H = \bigcup_c x_c(H \cap [c]H'),$$

where  $\{x_c\}$  is a family of elements of  $H$ , depending on  $c$ . Show that the elements  $\{x_cc\}$  form a family of left coset representatives for  $H'$  in  $G$ ; that is,

$$G = \bigcup_{x_c} \bigcup_{x_c} x_ccH',$$

and the union is disjoint. (Double cosets will not emerge further until Chapter XVIII.)

**Strategy:** For part (a), show that the relation  $x \sim y$  if and only if  $y \in HxH'$  is an equivalence relation. For part (b), use the decomposition of  $H$  into cosets of  $H \cap [c]H'$  and show that the resulting union gives all left cosets of  $H'$  in  $G$ .

**Solution:**

- (a) We show that the relation  $x \sim y$  if and only if  $y \in HxH'$  is an equivalence relation on  $G$ . Reflexivity:  $x \in HxH'$  since  $1 \in H$  and  $1 \in H'$ . Symmetry: if  $y \in HxH'$ , then  $y = h x h'$  for some  $h \in H$  and  $h' \in H'$ , so  $x = h^{-1} y h'^{-1} \in HyH'$ . Transitivity: if  $y \in HxH'$  and  $z \in HyH'$ , then  $y = h_1 x h'_1$  and  $z = h_2 y h'_2$  for some  $h_1, h_2 \in H$  and  $h'_1, h'_2 \in H'$ , so  $z = h_2 h_1 x h'_1 h'_2 \in HxH'$ . Therefore,  $G$  is the disjoint union of equivalence classes, which are the double cosets.
- (b) For each double coset representative  $c$ , we have  $H = \bigcup_{x_c} x_c(H \cap [c]H')$  where  $\{x_c\}$  are representatives for the cosets of  $H \cap [c]H'$  in  $H$ .

For any  $g \in G$ ,  $g$  lies in some double coset  $HcH'$  for some representative  $c$ . Then  $g = h c h'$  for some  $h \in H$  and  $h' \in H'$ . Since  $h \in H$ , we can write  $h = x_c k$  for some  $x_c$  and  $k \in H \cap [c]H'$ . Then  $g = x_c k c h' = x_c c (k^c h')$  where  $k^c = c^{-1} k c \in H'$  since  $k \in [c]H'$ . Therefore,  $g \in x_c c H'$ .

To show the union is disjoint, suppose  $x_c c H' \cap x_{c'} c' H' \neq \emptyset$  for some  $c, c'$  and some  $x_c, x_{c'}$ . Then  $x_c c h_1 = x_{c'} c' h_2$  for some

$h_1, h_2 \in H'$ . This implies  $x_{c'}^{-1}x_c c = c'h_2h_1^{-1} \in HcH' \cap Hc'H'$ . Since double cosets are disjoint, we must have  $c = c'$ , and then  $x_{c'}^{-1}x_c \in H \cap [c]H'$ , which means  $x_c$  and  $x_{c'}$  represent the same coset, so  $x_c = x_{c'}$ . ■

## 1.2 Normal Subgroups and Indices

### Key Definitions and Theorems:

**Definition:** The *index* of a subgroup  $H$  in  $G$ , denoted  $(G : H)$ , is the number of left cosets of  $H$  in  $G$ .

**Definition:** A *left coset* of  $H$  in  $G$  is a subset of the form  $gH = \{gh : h \in H\}$  for some  $g \in G$ .

**Definition:** A *right coset* of  $H$  in  $G$  is a subset of the form  $Hg = \{hg : h \in H\}$  for some  $g \in G$ .

**First Isomorphism Theorem:** If  $\phi : G \rightarrow H$  is a homomorphism, then  $G/\ker(\phi) \cong \text{im}(\phi)$ .

**Third Isomorphism Theorem:** If  $H$  and  $K$  are normal subgroups of  $G$  with  $H \subseteq K$ , then  $(G/H)/(K/H) \cong G/K$ .

**Definition:** The *kernel* of a homomorphism  $\phi : G \rightarrow H$  is  $\ker(\phi) = \{g \in G : \phi(g) = e_H\}$ .

**Definition:** The *image* of a homomorphism  $\phi : G \rightarrow H$  is  $\text{im}(\phi) = \{\phi(g) : g \in G\}$ .

**Theorem:** If  $H$  is a subgroup of finite index in  $G$ , then there exists a normal subgroup  $N$  of  $G$  contained in  $H$  and also of finite index.

**Theorem:** The number of left cosets equals the number of right cosets for any subgroup.

### 1.9: Subgroups of finite index

- (a) Let  $G$  be a group and  $H$  a subgroup of finite index. Show that there exists a normal subgroup  $N$  of  $G$  contained in  $H$  and also of finite index. [Hint: If  $(G : H) = n$ , find a homomorphism of  $G$  into  $S_n$  whose kernel is contained in  $H$ .]
- (b) Let  $G$  be a group and let  $H_1, H_2$  be subgroups of finite index. Prove that  $H_1 \cap H_2$  has finite index.

**Strategy:** For part (a), use the action of  $G$  on the left cosets of  $H$  to create a homomorphism into  $S_n$ . For part (b), use part (a) to find normal subgroups of finite index contained in each  $H_i$ , then use the fact that the intersection of subgroups of finite index has finite index.

**Solution:**

- (a) Let  $(G : H) = n$  and let  $\{g_1, \dots, g_n\}$  be a complete set of left coset representatives for  $H$  in  $G$ . Define an action of  $G$  on the set of left cosets  $\{g_1H, \dots, g_nH\}$  by  $g \cdot (g_iH) = gg_iH$ . This gives a homomorphism  $\phi : G \rightarrow S_n$  where  $\phi(g)$  is the permutation induced by the action of  $g$ .

The kernel  $N = \ker(\phi)$  consists of all elements  $g \in G$  such that  $gg_iH = g_iH$  for all  $i$ , which means  $g \in g_iHg_i^{-1}$  for all  $i$ . In particular,  $g \in H$  (when  $i = 1$ ), so  $N \subseteq H$ . Since  $G/N \cong \text{im}(\phi) \subseteq S_n$ , we have  $(G : N) \leq n! < \infty$ .

- (b) Let  $(G : H_1) = n_1$  and  $(G : H_2) = n_2$ . By part (a), there exist normal subgroups  $N_1 \subseteq H_1$  and  $N_2 \subseteq H_2$  with finite indices. Then  $N_1 \cap N_2 \subseteq H_1 \cap H_2$  and  $(G : N_1 \cap N_2) \leq (G : N_1)(G : N_2) < \infty$ , so  $H_1 \cap H_2$  has finite index.

■

### 1.10: Right and left cosets

Let  $G$  be a group and let  $H$  be a subgroup of finite index. Prove that there is only a finite number of right cosets of  $H$ , and that the number of right cosets is equal to the number of left cosets.

**Strategy:** Show that the inverses of left coset representatives form a complete set of right coset representatives. Use the fact that  $gH = Hg^{-1}$  to establish the correspondence.

**Solution:** Let  $(G : H) = n$  and let  $\{g_1, \dots, g_n\}$  be a complete set of left coset representatives. We show that  $\{g_1^{-1}, \dots, g_n^{-1}\}$  is a complete set of right coset representatives.

First, we show that every right coset  $Hg$  is equal to  $Hg_i^{-1}$  for some  $i$ . Since  $g \in g_iH$  for some  $i$ , we have  $g = g_ih$  for some  $h \in H$ . Then  $Hg = Hg_ih = Hg_i = Hg_i^{-1}$  (since  $g_iH = Hg_i^{-1}$ ).

Next, we show that the right cosets  $Hg_i^{-1}$  are distinct. If  $Hg_i^{-1} = Hg_j^{-1}$ , then  $g_i^{-1} \in Hg_j^{-1}$ , so  $g_i^{-1} = hg_j^{-1}$  for some  $h \in H$ . This implies  $g_i = g_jh^{-1} \in g_jH$ , which means  $g_iH = g_jH$ , so  $i = j$ .

Therefore, there are exactly  $n$  right cosets, and the number of right cosets equals the number of left cosets. ■

## 1.3 Group Actions

### Key Definitions and Theorems:

**Definition:** A *group action* of  $G$  on a set  $S$  is a function  $G \times S \rightarrow S$  (denoted  $(g, s) \mapsto g \cdot s$ ) such that:

1.  $e \cdot s = s$  for all  $s \in S$
2.  $(gh) \cdot s = g \cdot (h \cdot s)$  for all  $g, h \in G$  and  $s \in S$

**Definition:** The *orbit* of an element  $s \in S$  under the action of  $G$  is  $G \cdot s = \{g \cdot s : g \in G\}$ .

**Definition:** The *stabilizer* of an element  $s \in S$  is  $G_s = \{g \in G : g \cdot s = s\}$ .

**Orbit-Stabilizer Theorem:** If  $G$  acts on  $S$  and  $s \in S$ , then  $|G \cdot s| = (G : G_s)$ .

**Definition:** An action is *transitive* if there is only one orbit.

**Definition:** An action is *faithful* if the kernel of the action is trivial.

**Definition:** An action is *free* if every non-identity element has no fixed points.

**Class Equation:** For a finite group  $G$  acting on itself by conjugation,  $|G| = |Z(G)| + \sum |G|/|C(g)|$  where the sum is over representatives of non-central conjugacy classes.

**Definition:** A *fixed point* of an element  $g \in G$  is an element  $s \in S$  such that  $g \cdot s = s$ .

**Burnside's Lemma:** The number of orbits of a finite group  $G$  acting on a finite set  $S$  is  $\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$  where  $\text{Fix}(g)$  is the set of fixed points of  $g$ .

### 1.15: Fixed point free action

Let  $G$  be a finite group operating on a finite set  $S$  with  $\#(S) \geq 2$ . Assume that there is only one orbit. Prove that there exists an element  $x \in G$  which has no fixed point, i.e.  $xs \neq s$  for all  $s \in S$ .

**Strategy:** Use the class equation and the fact that the average number of fixed points over all elements of  $G$  is 1. Since the identity has more

than 1 fixed point, there must be some element with fewer than 1 fixed point.

**Solution:** Since there is only one orbit, the action is transitive. Let  $s_0 \in S$  and let  $H$  be the stabilizer of  $s_0$ . Then  $\#(S) = (G : H) = \#(G)/\#(H)$ .

For any  $g \in G$ , the number of fixed points of  $g$  is the number of elements  $s \in S$  such that  $gs = s$ . Since the action is transitive, for any  $s \in S$  there exists  $h \in G$  such that  $s = hs_0$ . Then  $gs = s$  if and only if  $ghs_0 = hs_0$ , which means  $h^{-1}gh \in H$ .

Therefore, the number of fixed points of  $g$  is equal to the number of conjugates of  $g$  that lie in  $H$ . By the class equation, the average number of fixed points over all elements of  $G$  is

$$\frac{1}{\#(G)} \sum_{g \in G} \text{fixed points of } g = \frac{1}{\#(G)} \sum_{g \in G} \#\{h \in G : h^{-1}gh \in H\} = \frac{\#(G)}{\#(G)} = 1.$$

Since  $\#(S) \geq 2$ , the identity element has  $\#(S) > 1$  fixed points. Therefore, there must exist some element  $x \in G$  with fewer than 1 fixed point, i.e., no fixed points. ■

### 1.16: Union of conjugates

Let  $H$  be a proper subgroup of a finite group  $G$ . Show that  $G$  is not the union of all the conjugates of  $H$ . (But see Exercise 23 of Chapter XIII.)

**Strategy:** Use the inclusion-exclusion principle and count the total number of elements in all conjugates. Show that this number exceeds  $|G|$  unless  $H$  is normal, in which case there's only one conjugate.

**Solution:** Let  $N = N_G(H)$  be the normalizer of  $H$  in  $G$ . The number of conjugates of  $H$  is  $(G : N)$ . Each conjugate of  $H$  has the same order  $\#(H)$ .

If  $G$  were the union of all conjugates of  $H$ , then by the inclusion-exclusion principle,

$$\#(G) \leq \sum_{g \in G/N} \#(gHg^{-1}) - \sum_{g_1, g_2 \in G/N, g_1 \neq g_2} \#(g_1Hg_1^{-1} \cap g_2Hg_2^{-1}) + \cdots$$

Since  $H$  is a proper subgroup,  $\#(H) < \#(G)$ . The first term in the sum is  $(G : N) \cdot \#(H)$ . Since  $(G : N) \geq 2$  (as  $H$  is proper), we have  $(G : N) \cdot \#(H) \geq 2\#(H) > \#(G)$  if  $\#(H) > \#(G)/2$ .

If  $\#(H) \leq \#(G)/2$ , then  $(G : N) \cdot \#(H) \leq \#(G) \cdot \#(H)/\#(H) = \#(G)$ , but this is only possible if  $(G : N) = 1$ , which means  $H$  is normal. In this case, there is only one conjugate of  $H$  (namely  $H$  itself), and  $H \neq G$  since  $H$  is proper.

Therefore,  $G$  cannot be the union of all conjugates of  $H$ . ■

### 1.19: Counting fixed points

Let  $G$  be a finite group operating on a finite set  $S$ .

- (a) For each  $s \in S$  show that

$$\sum_{i \in G_s} \frac{1}{\#(G_i)} = 1.$$

- (b) For each  $x \in G$  define  $f(x)$  = number of elements  $s \in S$  such that  $xs = s$ . Prove that the number of orbits of  $G$  in  $S$  is equal to

$$\frac{1}{\#(G)} \sum_{x \in G} f(x).$$

**Strategy:** For part (a), use the orbit-stabilizer theorem and count elements in the orbit. For part (b), use Burnside's lemma by counting fixed points and using the fact that each element stabilizes exactly one element in each orbit.

**Solution:**

- (a) For each  $s \in S$ , let  $G_s$  be the stabilizer of  $s$ . The orbit of  $s$  has size  $(G : G_s) = \#(G)/\#(G_s)$ .

For each  $g \in G$ , let  $G_g$  be the stabilizer of  $g \cdot s$ . Then  $G_g = gG_sg^{-1}$ , so  $\#(G_g) = \#(G_s)$ .

The sum  $\sum_{g \in G} \frac{1}{\#(G_g)}$  counts each element in the orbit of  $s$  exactly  $\#(G_s)$  times (once for each element in the stabilizer), divided by  $\#(G_s)$ . Therefore, this sum equals the size of the orbit, which is  $\#(G)/\#(G_s)$ .

But  $\sum_{g \in G} \frac{1}{\#(G_g)} = \sum_{g \in G} \frac{1}{\#(G_s)} = \#(G)/\#(G_s)$ , which equals the size of the orbit.

- (b) Let  $O_1, \dots, O_k$  be the orbits of  $G$  in  $S$ . For each orbit  $O_i$ , let  $s_i \in O_i$  and let  $G_i$  be the stabilizer of  $s_i$ . Then  $\#(O_i) = \#(G)/\#(G_i)$ .

For each  $x \in G$ , the number of fixed points of  $x$  is the sum over all orbits of the number of fixed points in each orbit. In orbit  $O_i$ ,  $x$  fixes  $s_i$  if and only if  $x \in G_i$ . Therefore,  $f(x) = \sum_{i=1}^k \chi_{G_i}(x)$ , where  $\chi_{G_i}$  is the characteristic function of  $G_i$ .

Then  $\sum_{x \in G} f(x) = \sum_{x \in G} \sum_{i=1}^k \chi_{G_i}(x) = \sum_{i=1}^k \sum_{x \in G} \chi_{G_i}(x) = \sum_{i=1}^k \#(G_i) = \sum_{i=1}^k \#(G)/\#(O_i) = \#(G) \sum_{i=1}^k 1/\#(O_i)$ .

But  $\sum_{i=1}^k 1/\#(O_i) = \sum_{i=1}^k \#(G_i)/\#(G) = \sum_{i=1}^k \#(G_i)/\#(G) = k$ , since each element of  $G$  stabilizes exactly one element in each orbit.

Therefore,  $\frac{1}{\#(G)} \sum_{x \in G} f(x) = k$ , the number of orbits.

■

## 1.4 Sylow Theory

### Key Definitions and Theorems:

**Definition:** A  $p$ -group is a group whose order is a power of a prime  $p$ .

**Definition:** A  $p$ -Sylow subgroup of a finite group  $G$  is a maximal  $p$ -subgroup of  $G$ .

**First Sylow Theorem:** If  $G$  is a finite group and  $p$  is a prime dividing  $|G|$ , then  $G$  contains a  $p$ -Sylow subgroup.

**Second Sylow Theorem:** All  $p$ -Sylow subgroups of  $G$  are conjugate to each other.

**Third Sylow Theorem:** The number  $n_p$  of  $p$ -Sylow subgroups satisfies  $n_p \equiv 1 \pmod{p}$  and  $n_p$  divides  $|G|$ .

**Definition:** The *centralizer*  $C_G(g)$  of an element  $g \in G$  is the set of elements that commute with  $g$ .

**Definition:** The *conjugacy class* of an element  $g \in G$  is the set  $\{hgh^{-1} : h \in G\}$ .

**Theorem:** If  $P$  is a  $p$ -Sylow subgroup of  $G$  and  $H$  is a  $p$ -subgroup of  $G$ , then  $H$  is contained in some conjugate of  $P$ .

**Theorem:** The center of a non-trivial  $p$ -group is non-trivial.

**Theorem:** If  $H$  is a normal subgroup of order  $p$  in a  $p$ -group  $G$ , then  $H$  is contained in the center of  $G$ .



**1.20: Center of  $p$ -group**

Let  $P$  be a  $p$ -group. Let  $A$  be a normal subgroup of order  $p$ . Prove that  $A$  is contained in the center of  $P$ .

**Strategy:** Consider the action of  $P$  on  $A$  by conjugation. Since  $A$  has order  $p$ , its automorphism group has order  $p - 1$ . Since  $P$  is a  $p$ -group, the action must be trivial, meaning  $A$  is central.

**Solution:** Since  $A$  is normal of order  $p$ , it is cyclic and generated by some element  $a$  of order  $p$ .

Consider the action of  $P$  on  $A$  by conjugation. Since  $A$  is normal, this action is well-defined. The kernel of this action is the centralizer  $C_P(A)$  of  $A$  in  $P$ .

Since  $A$  has order  $p$ , the automorphism group of  $A$  has order  $p - 1$ . Therefore, the image of  $P$  in  $\text{Aut}(A)$  has order dividing  $p - 1$ . But  $P$  is a  $p$ -group, so this image must be trivial.

This means that every element of  $P$  acts trivially on  $A$  by conjugation, i.e.,  $A \subseteq Z(P)$ , the center of  $P$ . ■

**1.21: Sylow intersections**

Let  $G$  be a finite group and  $H$  a subgroup. Let  $P_H$  be a  $p$ -Sylow subgroup of  $H$ . Prove that there exists a  $p$ -Sylow subgroup  $P$  of  $G$  such that  $P_H = P \cap H$ .

**Strategy:** Use Sylow's theorem to find a  $p$ -Sylow subgroup  $P$  of  $G$  containing  $P_H$ . Then show that  $P \cap H$  cannot be larger than  $P_H$  since  $P_H$  is already a maximal  $p$ -subgroup of  $H$ .

**Solution:** Let  $P$  be a  $p$ -Sylow subgroup of  $G$  containing  $P_H$ . Such a  $P$  exists because  $P_H$  is a  $p$ -subgroup of  $G$ , and by Sylow's theorem, it is contained in some  $p$ -Sylow subgroup of  $G$ .

Then  $P_H \subseteq P \cap H$ . Since  $P_H$  is a  $p$ -Sylow subgroup of  $H$ , it has the largest possible order among  $p$ -subgroups of  $H$ . But  $P \cap H$  is also a  $p$ -subgroup of  $H$ , so  $\#(P_H) \geq \#(P \cap H)$ .

Since  $P_H \subseteq P \cap H$  and  $\#(P_H) \geq \#(P \cap H)$ , we must have  $P_H = P \cap H$ . ■

**1.22: Normal subgroup in Sylow**

Let  $H$  be a normal subgroup of a finite group  $G$  and assume that  $\#(H) = p$ . Prove that  $H$  is contained in every  $p$ -Sylow subgroup of  $G$ .

**Strategy:** Use the fact that  $H$  is a  $p$ -subgroup and normal. By Sylow's theorem,  $H$  is contained in some  $p$ -Sylow subgroup, and since  $H$  is normal, it must be contained in all conjugates of that Sylow subgroup.

**Solution:** Since  $H$  is normal of order  $p$ , it is a  $p$ -subgroup of  $G$ . By Sylow's theorem,  $H$  is contained in some  $p$ -Sylow subgroup  $P$  of  $G$ .

Let  $P'$  be any other  $p$ -Sylow subgroup of  $G$ . By Sylow's theorem,  $P'$  is conjugate to  $P$ , so  $P' = gPg^{-1}$  for some  $g \in G$ .

Since  $H$  is normal,  $gHg^{-1} = H$ . Therefore,  $H = gHg^{-1} \subseteq gPg^{-1} = P'$ .

This shows that  $H$  is contained in every  $p$ -Sylow subgroup of  $G$ . ■

**1.23: Sylow normalizers**

Let  $P, P'$  be  $p$ -Sylow subgroups of a finite group  $G$ .

- (a) If  $P' \subseteq N(P)$  (normalizer of  $P$ ), then  $P' = P$ .
- (b) If  $N(P') = N(P)$ , then  $P' = P$ .
- (c) We have  $N(N(P)) = N(P)$ .

**Strategy:** For part (a), use the fact that if  $P'$  normalizes  $P$ , then  $PP'$  is a  $p$ -subgroup containing both  $P$  and  $P'$ . For part (b), use part (a). For part (c), show that any element normalizing  $N(P)$  must normalize  $P$  itself.

**Solution:**

- (a) If  $P' \subseteq N(P)$ , then  $P'$  normalizes  $P$ , so  $PP'$  is a subgroup of  $G$ . Since  $P$  and  $P'$  are both  $p$ -Sylow subgroups, they have the same order, and  $PP'$  is a  $p$ -subgroup containing both  $P$  and  $P'$ . By the maximality of  $p$ -Sylow subgroups, we must have  $PP' = P = P'$ .
- (b) If  $N(P') = N(P)$ , then  $P' \subseteq N(P') = N(P)$ . By part (a), this implies  $P' = P$ .

- (c) Let  $N = N(P)$ . Since  $P$  is normal in  $N$ ,  $P$  is the unique  $p$ -Sylow subgroup of  $N$ . If  $g \in N(N)$ , then  $g$  normalizes  $N$ , so  $gPg^{-1} \subseteq gNg^{-1} = N$ . Since  $gPg^{-1}$  is also a  $p$ -Sylow subgroup of  $N$ , we must have  $gPg^{-1} = P$ , which means  $g \in N(P) = N$ . Therefore,  $N(N) \subseteq N$ . The reverse inclusion is obvious, so  $N(N) = N$ . ■

## 1.5 Group Structure

### Key Definitions and Theorems:

**Definition:** A group is *solvable* if it has a subnormal series with abelian quotients.

**Definition:** A *subnormal series* is a sequence of subgroups  $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$  where each  $G_{i+1}$  is normal in  $G_i$ .

**Definition:** A group is *simple* if it has no non-trivial normal subgroups.

**Theorem:** Every group of order  $p^2$  is abelian.

**Theorem:** Every group of order  $pq$  where  $p < q$  are primes and  $q \not\equiv 1 \pmod{p}$  is cyclic.

**Theorem:** Every group of order less than 60 is solvable.

**Theorem:** Every group of order  $p^2q$  is solvable and has a normal Sylow subgroup.

**Theorem:** Every group of order  $2pq$  for odd primes  $p, q$  is solvable.

**Definition:** The *direct product* of groups  $G$  and  $H$  is  $G \times H = \{(g, h) : g \in G, h \in H\}$  with componentwise multiplication.

**Theorem:** If  $G$  and  $H$  are groups of coprime orders, then every subgroup of  $G \times H$  is of the form  $A \times B$  where  $A \leq G$  and  $B \leq H$ .

### 1.24: Groups of order $p^2$

Let  $p$  be a prime number. Show that a group of order  $p^2$  is abelian, and that there are only two such groups up to isomorphism.

**Strategy:** Use Lagrange's theorem to determine possible element orders. If there's an element of order  $p^2$ , the group is cyclic. Otherwise, show that every non-identity element has order  $p$  and construct an explicit isomorphism to  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

**Solution:** Let  $G$  be a group of order  $p^2$ . By Lagrange's theorem, every element has order 1,  $p$ , or  $p^2$ .

**Case 1:** If  $G$  has an element of order  $p^2$ , then  $G$  is cyclic and isomorphic to  $\mathbb{Z}_{p^2}$ .

**Case 2:** If every non-identity element has order  $p$ , then  $G$  is isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

To see this, let  $a \in G$  be any non-identity element. Since  $a$  has order  $p$ , the subgroup  $\langle a \rangle$  has order  $p$ . Let  $b \in G \setminus \langle a \rangle$ . Then  $b$  also has order  $p$ , and  $\langle a \rangle \cap \langle b \rangle = \{1\}$  since  $b \notin \langle a \rangle$ .

The subgroup  $\langle a, b \rangle$  has order  $p^2$  (since it contains all products  $a^i b^j$  for  $0 \leq i, j < p$ ), so  $G = \langle a, b \rangle$ . Since  $a$  and  $b$  commute (as we'll show),  $G$  is isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_p$ .

To show that  $a$  and  $b$  commute, consider the commutator  $[a, b] = aba^{-1}b^{-1}$ . Since  $G$  has order  $p^2$ , the center  $Z(G)$  is non-trivial (by the class equation). If  $[a, b] \neq 1$ , then  $\langle [a, b] \rangle$  is a non-trivial central subgroup, which contradicts the fact that  $a$  and  $b$  generate  $G$  and don't commute.

These are the only two possibilities, and they are non-isomorphic since  $\mathbb{Z}_{p^2}$  has an element of order  $p^2$  while  $\mathbb{Z}_p \times \mathbb{Z}_p$  does not. ■

### 1.25: Non-abelian groups of order $p^3$

Let  $G$  be a group of order  $p^3$ , where  $p$  is prime, and  $G$  is not abelian. Let  $Z$  be its center. Let  $C$  be a cyclic group of order  $p$ .

- (a) Show that  $Z \approx C$  and  $G/Z \approx C \times C$ .
- (b) Every subgroup of  $G$  of order  $p^2$  contains  $Z$  and is normal.
- (c) Suppose  $x^p = 1$  for all  $x \in G$ . Show that  $G$  contains a normal subgroup  $H \approx C \times C$ .

**Strategy:** For part (a), use the class equation to show  $Z$  has order  $p$ , then use the fact that  $G/Z$  cannot be cyclic since  $G$  is not abelian. For part (b), use the fact that  $Z$  is central and subgroups containing it are normal. For part (c), construct the subgroup using elements outside the center.

**Solution:**

- (a) Since  $G$  is not abelian,  $Z \neq G$ . By the class equation,  $Z$  is non-trivial. Since  $G$  is a  $p$ -group,  $Z$  has order  $p$  or  $p^2$ . If  $Z$  had order

$p^2$ , then  $G/Z$  would have order  $p$ , making it cyclic, which would imply  $G$  is abelian (contradiction). Therefore,  $Z \approx C$ .

Since  $G/Z$  has order  $p^2$  and is not cyclic (as  $G$  is not abelian), it must be isomorphic to  $C \times C$ .

- (b) Let  $H$  be a subgroup of order  $p^2$ . Since  $Z$  has order  $p$  and  $H$  has order  $p^2$ , we have  $Z \subseteq H$  (otherwise  $H \cap Z = \{1\}$  and  $HZ$  would have order  $p^3$ , which is impossible).

Since  $Z$  is central,  $H$  is normal if and only if  $gHg^{-1} = H$  for all  $g \in G$ . But  $gHg^{-1} = H$  since  $H$  contains  $Z$  and  $Z$  is central.

- (c) If  $x^p = 1$  for all  $x \in G$ , then every non-identity element has order  $p$ . Let  $a \in G \setminus Z$ . Then  $\langle a, Z \rangle$  is a subgroup of order  $p^2$  containing  $Z$ , so it is normal by part (b).

Let  $b \in G \setminus \langle a, Z \rangle$ . Then  $\langle b, Z \rangle$  is also a normal subgroup of order  $p^2$ . The intersection  $\langle a, Z \rangle \cap \langle b, Z \rangle = Z$  since  $b \notin \langle a, Z \rangle$ .

The subgroup  $H = \langle a, b, Z \rangle$  has order  $p^3$  (since it contains all products  $a^i b^j z$  for  $0 \leq i, j < p$  and  $z \in Z$ ), so  $H = G$ . Since  $a$  and  $b$  commute modulo  $Z$ ,  $G/Z \approx C \times C$  is generated by  $aZ$  and  $bZ$ , so  $H = \langle a, b \rangle \approx C \times C$ .

■

### 1.26: Groups of order $pq$

- (a) Let  $G$  be a group of order  $pq$ , where  $p, q$  are primes and  $p < q$ . Assume that  $q \not\equiv 1 \pmod{p}$ . Prove that  $G$  is cyclic.
- (b) Show that every group of order 15 is cyclic.

**Strategy:** Use Sylow's theorem to show that both Sylow subgroups are normal under the given conditions. Since they have trivial intersection and are both normal, the group is their direct product, which is cyclic.

**Solution:**

- (a) Let  $n_p$  and  $n_q$  be the number of  $p$ -Sylow and  $q$ -Sylow subgroups respectively. By Sylow's theorem,  $n_q \equiv 1 \pmod{q}$  and  $n_q$  divides  $p$ . Since  $p < q$ , we must have  $n_q = 1$ , so the  $q$ -Sylow subgroup is normal.

Similarly,  $n_p \equiv 1 \pmod{p}$  and  $n_p$  divides  $q$ . Since  $q \not\equiv 1 \pmod{p}$ , we must have  $n_p = 1$ , so the  $p$ -Sylow subgroup is normal.

Since  $P$  and  $Q$  are both normal and have trivial intersection,  $G = P \times Q \approx \mathbb{Z}_p \times \mathbb{Z}_q \approx \mathbb{Z}_{pq}$ .

- (b) For  $G$  of order 15, we have  $p = 3$  and  $q = 5$ . Since  $5 \not\equiv 1 \pmod{3}$ , the conditions of part (a) are satisfied, so  $G$  is cyclic. ■

### 1.27: Solvability of small groups

Show that every group of order  $< 60$  is solvable.

**Strategy:** Use the fact that  $A_5$  is the smallest non-solvable group and has order 60. For smaller orders, use known results about solvability of groups of specific orders and the fact that extensions of solvable groups by solvable groups are solvable.

**Solution:** We prove this by induction on the order. Groups of prime order are cyclic and hence solvable.

For composite orders, we use the fact that if a group has a normal subgroup and both the subgroup and quotient are solvable, then the group is solvable.

For orders less than 60, the only non-solvable group is  $A_5$  which has order 60. All other groups of order less than 60 are solvable because:

1. Groups of order  $p^n$  for prime  $p$  are  $p$ -groups and hence solvable.
2. Groups of order  $pq$  for primes  $p < q$  are solvable (they are either cyclic or have a normal  $q$ -Sylow subgroup).
3. Groups of order  $p^2q$  are solvable (they have a normal Sylow subgroup).
4. Groups of order  $p^3$  are solvable (they are  $p$ -groups).
5. Groups of order  $2pq$  for odd primes  $p, q$  are solvable.

The only remaining cases are orders 24, 36, 48, and 56, all of which have normal Sylow subgroups and are therefore solvable. ■

### 1.28: Groups of order $p^2q$

Let  $p, q$  be distinct primes. Prove that a group of order  $p^2q$  is solvable, and that one of its Sylow subgroups is normal.

**Strategy:** Use Sylow's theorem to analyze the possible numbers of Sylow subgroups. Show that in all cases, at least one Sylow subgroup must be normal, then use the fact that extensions of solvable groups by solvable groups are solvable.

**Solution:** Let  $G$  be a group of order  $p^2q$ . Let  $n_p$  and  $n_q$  be the number of  $p$ -Sylow and  $q$ -Sylow subgroups respectively.

By Sylow's theorem,  $n_q \equiv 1 \pmod{q}$  and  $n_q$  divides  $p^2$ . Therefore,  $n_q = 1$  or  $n_q = p$  or  $n_q = p^2$ .

If  $n_q = 1$ , then the  $q$ -Sylow subgroup is normal, and we're done.

If  $n_q = p$ , then  $p \equiv 1 \pmod{q}$ , which means  $q$  divides  $p-1$ . Since  $p$  and  $q$  are distinct primes, this is impossible unless  $p = 2$  and  $q = 3$ . In this case,  $G$  has order 12, and it can be shown that such groups have a normal Sylow subgroup.

If  $n_q = p^2$ , then  $p^2 \equiv 1 \pmod{q}$ , which means  $q$  divides  $(p-1)(p+1)$ . This is only possible if  $p = 2$  and  $q = 3$  or  $q = 5$ . In these cases, the groups can be analyzed directly and shown to have normal Sylow subgroups.

Therefore, one of the Sylow subgroups is normal. Since both Sylow subgroups are solvable (being  $p$ -groups and cyclic groups), and the quotient is also solvable,  $G$  is solvable. ■

### 1.29: Groups of order $2pq$

Let  $p, q$  be odd primes. Prove that a group of order  $2pq$  is solvable.

**Strategy:** Use Sylow's theorem to show that both the  $p$ -Sylow and  $q$ -Sylow subgroups are normal (since  $p$  and  $q$  are odd and greater than 2). Then use the fact that the product of two normal subgroups with trivial intersection is a normal subgroup.

**Solution:** Let  $G$  be a group of order  $2pq$ . Let  $n_2$ ,  $n_p$ , and  $n_q$  be the number of Sylow subgroups of orders 2,  $p$ , and  $q$  respectively.

By Sylow's theorem,  $n_q \equiv 1 \pmod{q}$  and  $n_q$  divides  $2p$ . Since  $q$  is odd and greater than 2, we must have  $n_q = 1$ , so the  $q$ -Sylow subgroup  $Q$  is normal.

Similarly,  $n_p \equiv 1 \pmod{p}$  and  $n_p$  divides  $2q$ . Since  $p$  is odd and greater than 2, we must have  $n_p = 1$ , so the  $p$ -Sylow subgroup  $P$  is normal.

Since both  $P$  and  $Q$  are normal and have trivial intersection,  $PQ$  is a normal subgroup of order  $pq$ . The quotient  $G/PQ$  has order 2, so it's cyclic and hence solvable.

Since  $P$  and  $Q$  are cyclic (being groups of prime order), they are solvable. Therefore,  $G$  is solvable. ■

### 1.30: Sylow in orders 40 and 12

- (a) Prove that one of the Sylow subgroups of a group of order 40 is normal.
- (b) Prove that one of the Sylow subgroups of a group of order 12 is normal.

**Strategy:** For each order, use Sylow's theorem to analyze the possible numbers of Sylow subgroups. For order 40, show the 5-Sylow subgroup is normal. For order 12, show that either the 2-Sylow or 3-Sylow subgroup must be normal by counting elements.

**Solution:**

- (a) Let  $G$  have order  $40 = 2^3 \cdot 5$ . Let  $n_2$  and  $n_5$  be the number of 2-Sylow and 5-Sylow subgroups respectively.

By Sylow's theorem,  $n_5 \equiv 1 \pmod{5}$  and  $n_5$  divides 8. Therefore,  $n_5 = 1$ , so the 5-Sylow subgroup is normal.

- (b) Let  $G$  have order  $12 = 2^2 \cdot 3$ . Let  $n_2$  and  $n_3$  be the number of 2-Sylow and 3-Sylow subgroups respectively.

By Sylow's theorem,  $n_3 \equiv 1 \pmod{3}$  and  $n_3$  divides 4. Therefore,  $n_3 = 1$  or  $n_3 = 4$ .

If  $n_3 = 1$ , then the 3-Sylow subgroup is normal.

If  $n_3 = 4$ , then there are 4 Sylow 3-subgroups, each containing 2 non-identity elements. These subgroups intersect only at the identity, so they account for 8 elements of order 3. The remaining 4 elements must form the unique 2-Sylow subgroup, so  $n_2 = 1$  and the 2-Sylow subgroup is normal.

In either case, one of the Sylow subgroups is normal. ■



**1.31: Groups of order  $\leq 10$** 

Determine all groups of order  $\leq 10$  up to isomorphism. In particular, show that a non-abelian group of order 6 is isomorphic to  $S_3$ .

**Strategy:** Use Lagrange's theorem and known classifications of small groups. For order 6, show that a non-abelian group must have elements of orders 2 and 3, and use the fact that  $S_3$  is the only non-abelian group of order 6.

**Solution:** We list all groups of order  $\leq 10$ :

**Order 1:** The trivial group.

**Order 2:**  $\mathbb{Z}_2$ .

**Order 3:**  $\mathbb{Z}_3$ .

**Order 4:**  $\mathbb{Z}_4$  and  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

**Order 5:**  $\mathbb{Z}_5$ .

**Order 6:**  $\mathbb{Z}_6$  and  $S_3$ . To see that a non-abelian group of order 6 is isomorphic to  $S_3$ , note that such a group must have elements of order 2 and 3. Let  $a$  be an element of order 3 and  $b$  an element of order 2. Since the group is non-abelian,  $ba \neq ab$ . The only possibility is  $ba = a^2b$ , which gives the presentation of  $S_3$ .

**Order 7:**  $\mathbb{Z}_7$ .

**Order 8:**  $\mathbb{Z}_8$ ,  $\mathbb{Z}_4 \times \mathbb{Z}_2$ ,  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ ,  $D_4$  (dihedral group), and  $Q_8$  (quaternion group).

**Order 9:**  $\mathbb{Z}_9$  and  $\mathbb{Z}_3 \times \mathbb{Z}_3$ .

**Order 10:**  $\mathbb{Z}_{10}$  and  $D_5$  (dihedral group).

The non-abelian groups are  $S_3$  (order 6),  $D_4$  (order 8),  $Q_8$  (order 8), and  $D_5$  (order 10). ■

## 1.6 Permutation Groups

### Key Definitions and Theorems:

**Definition:** The *symmetric group*  $S_n$  is the group of all permutations of  $\{1, 2, \dots, n\}$ .

**Definition:** A *cycle* of length  $k$  is a permutation that cyclically permutes  $k$  elements and fixes the rest.

**Definition:** A *transposition* is a cycle of length 2.

**Definition:** The *sign* of a permutation is  $(-1)^k$  where  $k$  is the number of transpositions in any decomposition.

**Definition:** A permutation is *even* if its sign is 1, *odd* if its sign is -1.

**Definition:** The *alternating group*  $A_n$  is the subgroup of  $S_n$  consisting of even permutations.

**Theorem:** Every permutation can be written as a product of disjoint cycles.

**Theorem:** Two permutations are conjugate in  $S_n$  if and only if they have the same cycle structure.

**Theorem:** The order of a cycle is its length.

**Theorem:** The conjugacy class of an  $n$ -cycle in  $S_n$  has  $(n-1)!$  elements.

**Theorem:** The centralizer of an  $n$ -cycle in  $S_n$  is the cyclic group generated by the cycle.

**Definition:** The *dihedral group*  $D_n$  is the group of symmetries of a regular  $n$ -gon.

**Definition:** The *quaternion group*  $Q_8$  is the group generated by  $i, j$  with relations  $i^4 = 1, j^4 = 1, i^2 = j^2, ij = -ji$ .

### 1.32: Sylow subgroups of symmetric groups

Let  $S_n$  be the permutation group on  $n$  elements. Determine the  $p$ -Sylow subgroups of  $S_3, S_4, S_5$  for  $p = 2$  and  $p = 3$ .

**Strategy:** Use the fact that Sylow subgroups of symmetric groups can be constructed from the action on the set. For 2-Sylow subgroups, use products of transpositions and 4-cycles. For 3-Sylow subgroups, use 3-cycles.

**Solution:** We determine the Sylow subgroups for each case:

$S_3$  (**order 6 = 2 · 3**): - 2-Sylow:  $\langle(12)\rangle$  or  $\langle(13)\rangle$  or  $\langle(23)\rangle$  (any transposition) - 3-Sylow:  $\langle(123)\rangle$  (the cyclic group of order 3)

$S_4$  (**order 24 = 2<sup>3</sup> · 3**): - 2-Sylow:  $\langle(12), (34)\rangle \cong D_4$  (dihedral group of order 8) - 3-Sylow:  $\langle(123)\rangle$  or  $\langle(124)\rangle$  or  $\langle(134)\rangle$  or  $\langle(234)\rangle$  (cyclic groups of order 3)

$S_5$  (**order 120 = 2<sup>3</sup> · 3 · 5**): - 2-Sylow:  $\langle(12), (34), (15)\rangle \cong D_4 \times \mathbb{Z}_2$  (order 16) - 3-Sylow:  $\langle(123)\rangle$  or any other 3-cycle (cyclic groups of order 3)

The 2-Sylow subgroups can be constructed by considering the action on the set and using the fact that they must be 2-groups. The 3-Sylow subgroups are always cyclic since they have prime order.

■

## 1.33: Sign of a permutation

Let  $\sigma$  be a permutation of a finite set  $I$  having  $n$  elements. Define  $e(\sigma)$  to be  $(-1)^m$  where

$$m = n - \text{number of orbits of } \sigma.$$

If  $I_1, \dots, I_r$  are the orbits of  $\sigma$ , then  $m$  is also equal to the sum

$$m = \sum_{v=1}^r [\text{card}(I_v) - 1].$$

If  $\tau$  is a transposition, show that  $e(\sigma\tau) = -e(\sigma)$  by considering the two cases when  $i, j$  lie in the same orbit of  $\sigma$ , or lie in different orbits. In the first case,  $\sigma\tau$  has one more orbit and in the second case one less orbit than  $\sigma$ . In particular, the sign of a transposition is  $-1$ . Prove that  $e(\sigma) = e(\sigma)$  is the sign of the permutation.

**Strategy:** Analyze how a transposition affects the number of orbits: it either splits one orbit into two or merges two orbits into one. Use this to show that  $e(\sigma\tau) = -e(\sigma)$ , then use the fact that any permutation is a product of transpositions.

**Solution:** Let  $\tau = (ij)$  be a transposition. We consider two cases:

**Case 1:**  $i$  and  $j$  lie in the same orbit of  $\sigma$ . Then  $\sigma\tau$  splits this orbit into two orbits, so the number of orbits increases by 1. Therefore,  $m$  decreases by 1, so  $e(\sigma\tau) = -e(\sigma)$ .

**Case 2:**  $i$  and  $j$  lie in different orbits of  $\sigma$ . Then  $\sigma\tau$  merges these two orbits into one, so the number of orbits decreases by 1. Therefore,  $m$  increases by 1, so  $e(\sigma\tau) = -e(\sigma)$ .

In both cases,  $e(\sigma\tau) = -e(\sigma)$ .

Since any permutation can be written as a product of transpositions, and each transposition changes the sign, we have  $e(\sigma) = (-1)^k$  where  $k$  is the number of transpositions in any decomposition of  $\sigma$ . This is exactly the sign of the permutation. ■

## 1.34: Dihedral groups

- (a) Let  $n$  be an even positive integer. Show that there exists a group of order  $2n$ , generated by two elements  $\sigma, \tau$  such that  $\sigma^n = e = \tau^2$ , and  $\sigma\tau = \tau\sigma^{n-1}$ . (Draw a picture of a regular  $n$ -gon, number the vertices, and use the picture as an inspiration to get  $\sigma, \tau$ .) This group is called the dihedral group.
- (b) Let  $n$  be an odd positive integer. Let  $D_{4n}$  be the group generated by the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

where  $\zeta$  is a primitive  $n$ -th root of unity. Show that  $D_{4n}$  has order  $4n$ , and give the commutation relations between the above generators.

**Strategy:** For part (a), use the geometric interpretation of the dihedral group as symmetries of a regular  $n$ -gon. For part (b), compute the orders of the matrices and their products to determine the group structure.

**Solution:**

- (a) Consider a regular  $n$ -gon with vertices numbered  $1, 2, \dots, n$  in clockwise order. Let  $\sigma$  be the rotation by  $2\pi/n$  radians (sending vertex  $i$  to vertex  $i+1 \bmod n$ ), and let  $\tau$  be the reflection across the line through vertex 1 and the center.

Then  $\sigma^n = e$  (rotation by  $2\pi$ ),  $\tau^2 = e$  (reflection twice), and  $\sigma\tau = \tau\sigma^{n-1}$  (this can be verified by checking the action on the vertices).

The group generated by  $\sigma$  and  $\tau$  has order  $2n$  because it contains the  $n$  rotations  $\sigma^i$  and the  $n$  reflections  $\sigma^i\tau$  for  $0 \leq i < n$ .

- (b) Let  $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ .

We have  $A^2 = -I$ ,  $A^4 = I$ , and  $B^n = I$ . Also,  $AB = \begin{pmatrix} 0 & -\zeta^{-1} \\ \zeta & 0 \end{pmatrix}$

and  $BA = \begin{pmatrix} 0 & -\zeta \\ \zeta^{-1} & 0 \end{pmatrix}$ .

Since  $n$  is odd,  $\zeta \neq \zeta^{-1}$ , so  $AB \neq BA$ . The group generated by  $A$  and  $B$  has order  $4n$  because it contains the  $4n$  elements  $A^i B^j$  for  $0 \leq i < 4$  and  $0 \leq j < n$ .

The commutation relation is  $AB = BA^{n-1}$ , which can be verified by direct computation. ■

### 1.35: Non-abelian groups of order 8

Show that there are exactly two non-isomorphic non-abelian groups of order 8. (One of them is given by generators  $\sigma, \tau$  with the relations

$$\sigma^4 = 1, \quad \tau^2 = 1, \quad \tau\sigma\tau = \sigma^3.$$

The other is the quaternion group.)

**Strategy:** Use the classification of groups of order 8. The only non-abelian groups are the dihedral group  $D_4$  and the quaternion group  $Q_8$ . Distinguish them by counting elements of order 2.

**Solution:** Let  $G$  be a non-abelian group of order 8. Since  $G$  is not abelian, it cannot be cyclic or isomorphic to  $\mathbb{Z}_4 \times \mathbb{Z}_2$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ .

The remaining possibilities are the dihedral group  $D_4$  and the quaternion group  $Q_8$ .

**Dihedral group  $D_4$ :** Generated by  $\sigma$  (rotation by  $\pi/2$ ) and  $\tau$  (reflection) with relations  $\sigma^4 = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^3$ .

**Quaternion group  $Q_8$ :** Generated by  $i$  and  $j$  with relations  $i^4 = 1, j^4 = 1, i^2 = j^2, ij = -ji$ .

These groups are non-isomorphic because  $D_4$  has 5 elements of order 2 (the reflections and the rotation by  $\pi$ ), while  $Q_8$  has only 1 element of order 2 (namely  $-1$ ). ■

### 1.36: Conjugacy class of $n$ -cycle

Let  $\sigma = [123 \cdots n]$  in  $S_n$ . Show that the conjugacy class of  $\sigma$  has  $(n-1)!$  elements. Show that the centralizer of  $\sigma$  is the cyclic group generated by  $\sigma$ .

**Strategy:** Use the fact that conjugacy classes in  $S_n$  are determined by cycle structure. Count the number of  $n$ -cycles by considering different starting positions. For the centralizer, show that only powers of  $\sigma$  can commute with it.

**Solution:** The conjugacy class of  $\sigma$  consists of all  $n$ -cycles. The number of  $n$ -cycles in  $S_n$  is  $(n-1)!$  because there are  $n!$  ways to arrange  $n$  elements, but each cycle can be written in  $n$  different ways (by starting at different positions).

The centralizer  $C(\sigma)$  consists of all permutations  $\tau$  such that  $\tau\sigma\tau^{-1} = \sigma$ . This means  $\tau$  must commute with  $\sigma$ .

Since  $\sigma$  is an  $n$ -cycle, any permutation that commutes with  $\sigma$  must be a power of  $\sigma$ . Therefore,  $C(\sigma) = \langle \sigma \rangle$ , which has order  $n$ .

By the orbit-stabilizer theorem, the size of the conjugacy class is  $|S_n|/|C(\sigma)| = n!/n = (n-1)!$ . ■

### 1.37: Conjugate cycles

- (a) Let  $\sigma = [i_1 \cdots i_m]$  be a cycle. Let  $\gamma \in S_n$ . Show that  $\gamma\sigma\gamma^{-1}$  is the cycle  $[\gamma(i_1) \cdots \gamma(i_m)]$ .
- (b) Suppose that a permutation  $\sigma$  in  $S_n$  can be written as a product of  $r$  disjoint cycles, and let  $d_1, \dots, d_r$  be the number of elements in each cycle, in increasing order. Let  $\tau$  be another permutation which can be written as a product of disjoint cycles, whose cardinalities are  $d'_1, \dots, d'_s$  in increasing order. Prove that  $\sigma$  is conjugate to  $\tau$  in  $S_n$  if and only if  $r = s$  and  $d_i = d'_i$  for all  $i = 1, \dots, r$ .

**Strategy:** For part (a), verify the action of  $\gamma\sigma\gamma^{-1}$  on the elements  $\gamma(i_j)$ . For part (b), use part (a) to show that conjugate permutations have the same cycle structure, then construct a permutation that conjugates one to the other.

**Solution:**

- (a) Let  $\sigma = [i_1 \cdots i_m]$  and let  $\gamma \in S_n$ . We show that  $\gamma\sigma\gamma^{-1} = [\gamma(i_1) \cdots \gamma(i_m)]$ .

For any  $j \in \{1, \dots, n\}$ , we have: - If  $j = \gamma(i_k)$  for some  $k$ , then  $\gamma\sigma\gamma^{-1}(j) = \gamma\sigma(i_k) = \gamma(i_{k+1 \bmod m})$ . - If  $j \neq \gamma(i_k)$  for any  $k$ , then

$\gamma^{-1}(j) \notin \{i_1, \dots, i_m\}$ , so  $\sigma\gamma^{-1}(j) = \gamma^{-1}(j)$ , and thus  $\gamma\sigma\gamma^{-1}(j) = j$ .

This shows that  $\gamma\sigma\gamma^{-1}$  acts as the cycle  $[\gamma(i_1) \cdots \gamma(i_m)]$ .

- (b) The "only if" direction follows from part (a): if  $\sigma$  and  $\tau$  are conjugate, then they have the same cycle structure.

For the "if" direction, suppose  $\sigma$  and  $\tau$  have the same cycle structure. Write  $\sigma = \sigma_1 \cdots \sigma_r$  and  $\tau = \tau_1 \cdots \tau_r$  as products of disjoint cycles, where  $\sigma_i$  and  $\tau_i$  have the same length  $d_i$ .

For each  $i$ , let  $\gamma_i$  be a permutation that maps the elements of  $\sigma_i$  to the elements of  $\tau_i$  in the same order. Then  $\gamma = \gamma_1 \cdots \gamma_r$  (where the  $\gamma_i$  act on disjoint sets) satisfies  $\gamma\sigma\gamma^{-1} = \tau$ .

■

### 1.38: Generating symmetric groups

- (a) Show that  $S_n$  is generated by the transpositions  $[12], [13], \dots, [1n]$ .
- (b) Show that  $S_n$  is generated by the transpositions  $[12], [23], [34], \dots, [n-1, n]$ .
- (c) Show that  $S_n$  is generated by the cycles  $[12]$  and  $[123 \dots n]$ .
- (d) Assume that  $n$  is prime. Let  $\sigma = [123 \dots n]$  and let  $\tau = [rs]$  be any transposition. Show that  $\sigma, \tau$  generate  $S_n$ .

**Strategy:** For parts (a) and (b), show that any transposition can be written in terms of the given generators. For part (c), use conjugation by the  $n$ -cycle to generate adjacent transpositions. For part (d), use the fact that  $n$  is prime to show that conjugates of  $\tau$  by powers of  $\sigma$  generate all transpositions.

**Solution:**

- (a) Any permutation can be written as a product of transpositions. Any transposition  $[ij]$  with  $i, j \neq 1$  can be written as  $[1i][1j][1i]$ . Therefore, the transpositions  $[12], [13], \dots, [1n]$  generate all transpositions, and hence generate  $S_n$ .
- (b) Any transposition  $[ij]$  can be written as a product of adjacent transpositions. For example,  $[13] = [12][23][12]$ ,  $[14] = [12][23][34][23][12]$ ,

etc. Therefore, the adjacent transpositions generate all transpositions, and hence generate  $S_n$ .

- (c) Let  $\sigma = [12]$  and  $\rho = [123 \dots n]$ . We show that any transposition can be written in terms of  $\sigma$  and  $\rho$ .

For any  $i \neq 1$ , we have  $\rho^{i-1}\sigma\rho^{-(i-1)} = [i, i+1]$ . Therefore, we can generate all adjacent transpositions, and hence all transpositions by part (b).

- (d) Since  $n$  is prime,  $\sigma$  is an  $n$ -cycle and has order  $n$ . The subgroup generated by  $\sigma$  and  $\tau$  contains  $\tau$  and all conjugates of  $\tau$  by powers of  $\sigma$ .

Since  $\tau = [rs]$ , the conjugates  $\sigma^i\tau\sigma^{-i}$  for  $0 \leq i < n$  give us all transpositions of the form  $[r+i, s+i]$  (where addition is modulo  $n$ ).

Since  $n$  is prime, these conjugates generate all transpositions, and hence generate  $S_n$ .

■

## 1.7 Alternating Groups

### Key Definitions and Theorems:

**Definition:** The *alternating group*  $A_n$  is the subgroup of  $S_n$  consisting of even permutations.

**Definition:** An action is *k-transitive* if for any two ordered  $k$ -tuples of distinct elements, there exists a group element mapping one to the other.

**Definition:** An action is *primitive* if the only stable partitions are the trivial ones.

**Definition:** A *stable partition* under a group action is a partition that is preserved by the group action.

**Theorem:**  $A_n$  is  $(n-2)$ -transitive for  $n \geq 3$ .

**Theorem:**  $A_n$  is simple for  $n \geq 5$ .

**Theorem:**  $A_5$  is the smallest non-abelian simple group.

**Theorem:** If  $H$  is a subgroup of index  $n$  in  $A_n$ , then the action of  $A_n$  on cosets of  $H$  gives an isomorphism  $A_n \rightarrow A_n$ .

**Theorem:** Any simple group of order 60 is isomorphic to  $A_5$ .

**Definition:** A *maximal subgroup* is a proper subgroup that is not contained in any larger proper subgroup.

**Theorem:** A group action is primitive if and only if the stabilizer of any point is a maximal subgroup.



**1.39: Transitivity of alternating group**

Show that the action of the alternating group  $A_n$  on  $\{1, \dots, n\}$  is  $(n-2)$ -transitive.

**Strategy:** Use the fact that  $S_n$  is  $n$ -transitive and show that for any  $(n-2)$ -tuple mapping, there exists an even permutation that does the job. If the permutation is odd, compose it with a transposition of the remaining two elements.

**Solution:** We need to show that for any two ordered  $(n-2)$ -tuples  $(a_1, \dots, a_{n-2})$  and  $(b_1, \dots, b_{n-2})$  of distinct elements, there exists  $\sigma \in A_n$  such that  $\sigma(a_i) = b_i$  for all  $i$ .

Let  $c_1, c_2$  be the remaining two elements not in the first tuple, and  $d_1, d_2$  be the remaining two elements not in the second tuple.

There exists a permutation  $\tau \in S_n$  such that  $\tau(a_i) = b_i$  for all  $i$ ,  $\tau(c_1) = d_1$ , and  $\tau(c_2) = d_2$ .

If  $\tau$  is even, we're done. If  $\tau$  is odd, then the permutation  $\tau' = \tau \circ (d_1 d_2)$  is even and satisfies  $\tau'(a_i) = b_i$  for all  $i$ .

Therefore,  $A_n$  is  $(n-2)$ -transitive. ■

**1.40: Subgroups of index  $n$  in  $A_n$** 

Let  $A_n$  be the alternating group of even permutations of  $\{1, \dots, n\}$ . For  $j = 1, \dots, n$  let  $H_j$  be the subgroup of  $A_n$  fixing  $j$ , so  $H_j \approx A_{n-1}$ , and  $(A_n : H_j) = n$  for  $n \geq 3$ . Let  $n \geq 3$  and let  $H$  be a subgroup of index  $n$  in  $A_n$ .

- (a) Show that the action of  $A_n$  on cosets of  $H$  by left translation gives an isomorphism  $A_n$  with the alternating group of permutations of  $A_n/H$ .
- (b) Show that there exists an automorphism of  $A_n$  mapping  $H_1$  on  $H$ , and that such an automorphism is induced by an inner automorphism of  $S_n$  if and only if  $H = H_i$  for some  $i$ .

**Strategy:** For part (a), use the fact that  $A_n$  is simple for  $n \geq 5$  to show the action is faithful, then use the order to show the image is  $A_n$ . For part (b), use the action to construct an automorphism and analyze when it's inner.

**Solution:**

- (a) The action of  $A_n$  on the cosets of  $H$  by left translation gives a homomorphism  $\phi : A_n \rightarrow S_n$  (since there are  $n$  cosets).

The kernel of  $\phi$  is the intersection of all conjugates of  $H$ , which is a normal subgroup of  $A_n$ . Since  $A_n$  is simple for  $n \geq 5$ , the kernel is trivial, so  $\phi$  is injective.

The image of  $\phi$  is a subgroup of  $S_n$  of index 2 (since  $|A_n| = n!/2$ ), so it must be  $A_n$ . Therefore,  $\phi$  is an isomorphism.

- (b) Since  $H$  has index  $n$  in  $A_n$ , the action of  $A_n$  on  $A_n/H$  gives an isomorphism  $A_n \rightarrow A_n$ . This isomorphism maps  $H_1$  to  $H$ .

If  $H = H_i$  for some  $i$ , then the automorphism is induced by conjugation by the transposition  $(1i)$  in  $S_n$ .

Conversely, if the automorphism is induced by an inner automorphism of  $S_n$ , then it is conjugation by some element of  $S_n$ . Since  $A_n$  is normal in  $S_n$ , this conjugation maps  $H_1$  to some  $H_i$ .

■

**1.41: Simple group of order 60**

Let  $H$  be a simple group of order 60.

- (a) Show that the action of  $H$  by conjugation on the set of its Sylow subgroups gives an imbedding  $H \subseteq A_6$ .
- (b) Using the preceding exercise, show that  $H \approx A_5$ .
- (c) Show that  $A_6$  has an automorphism which is not induced by an inner automorphism of  $S_6$ .

**Strategy:** For part (a), use Sylow's theorem to count Sylow subgroups and show the action gives an embedding. For part (b), use the previous exercise to show  $H$  has index 6 in  $A_6$ . For part (c), use the automorphism from the previous exercise.

**Solution:**

- (a) Let  $H$  be a simple group of order 60. The prime factorization is  $60 = 2^2 \cdot 3 \cdot 5$ .

Let  $n_2$ ,  $n_3$ , and  $n_5$  be the number of Sylow subgroups of orders 4, 3, and 5 respectively.

By Sylow's theorem,  $n_5 \equiv 1 \pmod{5}$  and  $n_5$  divides 12, so  $n_5 = 1$  or  $n_5 = 6$ . Since  $H$  is simple,  $n_5 = 6$ .

Similarly,  $n_3 \equiv 1 \pmod{3}$  and  $n_3$  divides 20, so  $n_3 = 1$  or  $n_3 = 4$  or  $n_3 = 10$ . Since  $H$  is simple,  $n_3 = 10$ .

The action of  $H$  by conjugation on the set of Sylow 5-subgroups gives a homomorphism  $H \rightarrow S_6$ . Since  $H$  is simple, this homomorphism is injective, so  $H$  embeds into  $S_6$ .

Since  $H$  has order 60 and  $A_6$  has order 360,  $H$  embeds into  $A_6$ .

- (b) By the previous exercise, any subgroup of index 6 in  $A_6$  is isomorphic to  $A_5$ . Since  $H$  has order 60 and  $A_6$  has order 360,  $H$  has index 6 in  $A_6$ , so  $H \approx A_5$ .
- (c) The automorphism of  $A_6$  that maps  $H_1$  to  $H_2$  (where  $H_i$  is the stabilizer of  $i$ ) is not induced by an inner automorphism of  $S_6$  because it maps  $H_1$  to  $H_2$  instead of to  $H_1$ .

■

## 1.8 Abelian Groups

### Key Definitions and Theorems:

**Definition:** An *abelian group* is a group where the operation is commutative.

**Definition:** A *torsion group* is a group where every element has finite order.

**Definition:** A *torsion-free group* is a group where only the identity has finite order.

**Definition:** A *mixed group* is a group that is neither torsion nor torsion-free.

**Fundamental Theorem of Finite Abelian Groups:** Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders.

**Structure Theorem for Finitely Generated Abelian Groups:** Every finitely generated abelian group is isomorphic to  $\mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$  where  $r \geq 0$  and  $n_i$  are powers of primes.

**Definition:** The *rank* of a finitely generated abelian group is the number of copies of  $\mathbb{Z}$  in its decomposition.

**Theorem:**  $\mathbb{Q}/\mathbb{Z}$  is a torsion group with exactly one subgroup of order  $n$  for each positive integer  $n$ .

**Theorem:** Every finite abelian group has a subgroup isomorphic to any given quotient.

**Definition:** The *Herbrand quotient* of a finite cyclic group  $G$  acting on an abelian group  $A$  is  $q(A) = (A_f : A^g)(A_g : A^f)$  where  $f(x) = \sigma x - x$  and  $g(x) = x + \sigma x + \cdots + \sigma^{n-1}x$ .

#### 1.42: Torsion group $\mathbb{Q}/\mathbb{Z}$

Viewing  $\mathbb{Z}, \mathbb{Q}$  as additive groups, show that  $\mathbb{Q}/\mathbb{Z}$  is a torsion group, which has one and only one subgroup of order  $n$  for each integer  $n \geq 1$ , and that this subgroup is cyclic.

**Strategy:** Show that every element has finite order by writing rational numbers as fractions. For the subgroup of order  $n$ , show that  $\langle \frac{1}{n} + \mathbb{Z} \rangle$  is the unique cyclic subgroup of order  $n$ .

**Solution:** First, we show that  $\mathbb{Q}/\mathbb{Z}$  is a torsion group. For any  $q \in \mathbb{Q}$ , we can write  $q = a/b$  where  $a, b \in \mathbb{Z}$  and  $b > 0$ . Then  $bq = a \in \mathbb{Z}$ , so  $b(q + \mathbb{Z}) = a + \mathbb{Z} = \mathbb{Z}$  in  $\mathbb{Q}/\mathbb{Z}$ . Therefore, every element has finite order.

For any integer  $n \geq 1$ , the subgroup of  $\mathbb{Q}/\mathbb{Z}$  of order  $n$  is  $\langle \frac{1}{n} + \mathbb{Z} \rangle$ . This subgroup is cyclic and has exactly  $n$  elements:  $\frac{k}{n} + \mathbb{Z}$  for  $0 \leq k < n$ .

To show uniqueness, suppose  $H$  is another subgroup of order  $n$ . Let  $q + \mathbb{Z}$  be a generator of  $H$ . Then  $n(q + \mathbb{Z}) = \mathbb{Z}$ , so  $nq \in \mathbb{Z}$ . This means  $q = \frac{k}{n}$  for some  $k \in \mathbb{Z}$ . Since  $H$  has order  $n$ , we must have  $\gcd(k, n) = 1$ , so  $H = \langle \frac{1}{n} + \mathbb{Z} \rangle$ . ■

#### 1.43: Subgroup isomorphic to quotient

Let  $H$  be a subgroup of a finite abelian group  $G$ . Show that  $G$  has a subgroup that is isomorphic to  $G/H$ .

**Strategy:** Use the fundamental theorem of finite abelian groups to decompose  $G$  and  $H$  into direct products of cyclic groups. Then construct a subgroup isomorphic to  $G/H$  using the appropriate factors.

**Solution:** Since  $G$  is a finite abelian group, it is isomorphic to a direct product of cyclic groups of prime power orders:  $G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$ .

The subgroup  $H$  corresponds to a subgroup of this direct product, which is also a direct product of cyclic groups:  $H \cong \mathbb{Z}_{p_1^{b_1}} \times \cdots \times \mathbb{Z}_{p_k^{b_k}}$  where  $0 \leq b_i \leq a_i$ .

The quotient  $G/H$  is isomorphic to  $\mathbb{Z}_{p_1^{a_1-b_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k-b_k}}$ .

The subgroup of  $G$  isomorphic to  $G/H$  is  $\mathbb{Z}_{p_1^{a_1-b_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k-b_k}} \times \{0\} \times \cdots \times \{0\}$ . ■

#### 1.44: Index formula

Let  $f : A \rightarrow A'$  be a homomorphism of abelian groups. Let  $B$  be a subgroup of  $A$ . Denote by  $A'$  and  $A_f$  the image and kernel of  $f$  in  $A$  respectively, and similarly for  $B'$  and  $B_f$ . Show that  $(A : B) = (A' : B')(A_f : B_f)$ , in the sense that if two of these three indices are finite, so is the third, and the stated equality holds.

**Strategy:** Use the isomorphism theorems to relate the indices. Apply the first isomorphism theorem to  $A/A_f \cong A'$  and  $B/B_f \cong B'$ , then use the third isomorphism theorem.

**Solution:** We use the isomorphism theorems for abelian groups.

By the first isomorphism theorem,  $A/A_f \cong A'$  and  $B/B_f \cong B'$ .

By the third isomorphism theorem,  $(A/A_f)/(B/B_f) \cong A/B$ .

Therefore,  $(A : B) = |A/B| = |(A/A_f)/(B/B_f)| = |A/A_f|/|B/B_f| = |A'|/|B'| = (A' : B')$ .

Also,  $(A_f : B_f) = |A_f/B_f| = |A_f|/|B_f|$ .

Since  $A_f \subseteq A$  and  $B_f \subseteq B$ , we have  $(A : B) = (A' : B')(A_f : B_f)$ . ■

#### 1.45: Herbrand quotient

Let  $G$  be a finite cyclic group of order  $n$ , generated by an element  $\sigma$ . Assume that  $G$  operates on an abelian group  $A$ , and let  $f, g : A \rightarrow A$  be the endomorphisms of  $A$  given by

$$f(x) = \sigma x - x \quad \text{and} \quad g(x) = x + \sigma x + \cdots + \sigma^{n-1}x.$$

Define the Herbrand quotient by the expression  $q(A) = (A_f : A^g)(A_g : A^f)$ , provided both indices are finite. Assume now that  $B$  is a subgroup of  $A$  such that  $GB \subset B$ .

(a) Define in a natural way an operation of  $G$  on  $A/B$ .

(b) Prove that

$$q(A) = q(B)q(A/B)$$

in the sense that if two of these quotients are finite, so is the third, and the stated equality holds.

(c) If  $A$  is finite, show that  $q(A) = 1$ .

(This exercise is a special case of the general theory of Euler characteristics discussed in Chapter XX, Theorem 3.1. After reading this, the present exercise becomes trivial. Why?)

**Strategy:** For part (a), define the action by  $\sigma \cdot (a + B) = \sigma a + B$ . For part (b), use exact sequences and the snake lemma to relate the quotients. For part (c), use part (b) with  $B = \{0\}$ .

**Solution:**

(a) The operation of  $G$  on  $A/B$  is defined by  $\sigma \cdot (a + B) = \sigma a + B$ . This is well-defined because  $GB \subset B$ .

(b) We have the following exact sequences:

$$0 \rightarrow B_f \rightarrow A_f \rightarrow (A/B)_f \rightarrow 0$$

and

$$0 \rightarrow B^g \rightarrow A^g \rightarrow (A/B)^g \rightarrow 0$$

By the snake lemma, we have exact sequences:

$$0 \rightarrow B_f \rightarrow A_f \rightarrow (A/B)_f \rightarrow B^g/B_f \rightarrow A^g/A_f \rightarrow (A/B)^g/(A/B)_f \rightarrow 0$$

This gives us the relation:

$$(A_f : A^g) = (B_f : B^g)((A/B)_f : (A/B)^g)$$

Therefore,  $q(A) = q(B)q(A/B)$ .

- (c) If  $A$  is finite, then all the groups involved are finite, so all indices are finite. By part (b),  $q(A) = q(B)q(A/B)$  for any  $G$ -invariant subgroup  $B$ .

Taking  $B = \{0\}$ , we have  $q(A) = q(\{0\})q(A) = 1 \cdot q(A)$ , so  $q(A) = 1$ .

■

## 1.9 Primitive Groups

### Key Definitions and Theorems:

**Definition:** A group action is *primitive* if the only stable partitions are the trivial ones (the whole set and singletons).

**Definition:** A *stable partition* under a group action is a partition that is preserved by the group action.

**Definition:** A *maximal subgroup* is a proper subgroup that is not contained in any larger proper subgroup.

**Theorem:** A group action is primitive if and only if the stabilizer of any point is a maximal subgroup.

**Definition:** An action is *doubly transitive* if it is 2-transitive.

**Theorem:** A group is doubly transitive if and only if the stabilizer of a point acts transitively on the remaining points.

**Theorem:** If  $G$  is doubly transitive and  $(G : H) = n$ , then  $|G| = d(n-1)n$  where  $d$  is the order of the subgroup fixing two points.

**Theorem:** A doubly transitive group is primitive.

**Definition:** The *isotropy group* or *stabilizer* of a point  $s$  is  $G_s = \{g \in G : g \cdot s = s\}$ .

**Theorem:** For a transitive action,  $\sum_{x \in G} f(x) = |G|$  where  $f(x)$  is the number of fixed points of  $x$ .

**Theorem:** A group is doubly transitive if and only if  $\sum_{x \in G} f(x)^2 = 2|G|$ .

### 1.46: Primitive group conditions

Let  $G$  operate on a set  $S$ . Let  $S = \bigcup S_i$  be a partition of  $S$  into disjoint subsets. We say that the partition is stable under  $G$  if  $G$  maps each  $S_i$  onto  $S_j$  for some  $j$ , and hence  $G$  induces a permutation of the sets of the partition among themselves. There are two partitions of  $S$  which are obviously stable: the partition consisting of  $S$  itself, and

the partition consisting of the subsets with one element. Assume that  $G$  operates transitively, and that  $S$  has more than one element. Prove that the following two conditions are equivalent:

PRIM 1. The only partitions of  $S$  which are stable are the two partitions mentioned above.

PRIM 2. If  $H$  is the isotropy group of an element of  $S$ , then  $H$  is a maximal subgroup of  $G$ .

These two conditions define what is known as a primitive group, or more accurately, a primitive operation of  $G$  on  $S$ .

**Strategy:** For PRIM 1  $\Rightarrow$  PRIM 2, assume  $H$  is not maximal and construct a non-trivial stable partition. For PRIM 2  $\Rightarrow$  PRIM 1, assume there's a non-trivial stable partition and show  $H$  is not maximal.

**Solution:** We prove the equivalence of PRIM 1 and PRIM 2.

**PRIM 1  $\Rightarrow$  PRIM 2:** Let  $H$  be the isotropy group of an element  $s \in S$ . Suppose  $H$  is not maximal, so there exists a subgroup  $K$  with  $H \subsetneq K \subsetneq G$ .

Let  $S' = \{gs : g \in K\}$ . Since  $H \subset K$ ,  $S'$  contains  $s$ . Since  $K \neq G$  and the action is transitive,  $S' \neq S$ . Since  $K \neq H$ ,  $S'$  contains more than one element.

The partition  $\{S', S \setminus S'\}$  is stable under  $G$  because for any  $g \in G$ , either  $gK = K$  (in which case  $gS' = S'$ ) or  $gK \cap K = H$  (in which case  $gS' \cap S' = \{s\}$  and  $gS' \subseteq S \setminus S'$ ).

This contradicts PRIM 1, so  $H$  must be maximal.

**PRIM 2  $\Rightarrow$  PRIM 1:** Let  $H$  be the isotropy group of an element  $s \in S$ . Suppose there exists a stable partition  $\{S_1, \dots, S_k\}$  with  $1 < k < |S|$ .

Let  $s \in S_1$ . The subgroup  $K = \{g \in G : gS_1 = S_1\}$  contains  $H$  and is a proper subgroup of  $G$  (since the action is transitive).

Since  $H \subsetneq K \subsetneq G$ ,  $H$  is not maximal, contradicting PRIM 2.

Therefore, the only stable partitions are the trivial ones. ■

### 1.47: Double transitivity

Let a finite group  $G$  operate transitively and faithfully on a set  $S$  with at least 2 elements and let  $H$  be the isotropy group of some element



$s$  of  $S$ . (All the other isotropy groups are conjugates of  $H$ .) Prove the following:

- (a)  $G$  is doubly transitive if and only if  $H$  acts transitively on the complement of  $s$  in  $S$ .
- (b)  $G$  is doubly transitive if and only if  $G = HTH$ , where  $T$  is a subgroup of  $G$  of order 2 not contained in  $H$ .
- (c) If  $G$  is doubly transitive, and  $(G : H) = n$ , then

$$\#(G) = d(n-1)n,$$

where  $d$  is the order of the subgroup fixing two elements. Furthermore,  $H$  is a maximal subgroup of  $G$ , i.e.  $G$  is primitive.

**Strategy:** For part (a), use the definition of double transitivity and the fact that  $G$  is transitive. For part (b), use the double coset decomposition. For part (c), use the orbit-stabilizer theorem and the fact that double transitive groups are primitive.

**Solution:**

- (a)  $G$  is doubly transitive if and only if for any two pairs  $(s_1, s_2)$  and  $(t_1, t_2)$  of distinct elements, there exists  $g \in G$  such that  $gs_1 = t_1$  and  $gs_2 = t_2$ .

Since  $G$  is transitive, we can assume  $s_1 = s$ . Then  $G$  is doubly transitive if and only if for any  $s_2 \neq s$  and any  $t_1, t_2 \in S$  with  $t_1 \neq t_2$ , there exists  $g \in G$  such that  $gs = t_1$  and  $gs_2 = t_2$ .

This is equivalent to  $H$  acting transitively on  $S \setminus \{s\}$ .

- (b) If  $G$  is doubly transitive, then for any  $t \in S \setminus \{s\}$ , there exists  $g \in G$  such that  $gs = s$  and  $gt = t'$  for some  $t' \neq s$ . This means  $g \in H$  and  $g \notin H$ .

Let  $T = \langle g \rangle$  where  $g$  is such an element. Then  $T$  has order 2 and is not contained in  $H$ .

Since  $G$  is transitive,  $G = \bigcup_{t \in S} HtH = HTH$ .

Conversely, if  $G = HTH$  where  $T$  has order 2 and is not contained in  $H$ , then  $T$  contains an element that maps  $s$  to some other element, and  $H$  acts transitively on the complement of  $s$ .

- (c) If  $G$  is doubly transitive, then the stabilizer of two points has order  $d = \#(G)/(n(n-1))$ .

Since  $G$  is doubly transitive, it is primitive by part (a) and the previous exercise, so  $H$  is maximal. ■

### 1.48: Counting fixed points

Let  $G$  be a group acting transitively on a set  $S$  with at least 2 elements. For each  $x \in G$  let  $f(x)$  = number of elements of  $S$  fixed by  $x$ . Prove:

- (a)  $\sum_{x \in G} f(x) = \#(G)$ .
- (b)  $G$  is doubly transitive if and only if

$$\sum_{x \in G} f(x)^2 = 2\#(G).$$

**Strategy:** For part (a), use the fact that each element stabilizes exactly one element in each orbit. For part (b), use the fact that in a doubly transitive action, each element fixes either 0 or 1 ordered pairs of distinct elements.

**Solution:**

- (a) Let  $s \in S$  and let  $H$  be the stabilizer of  $s$ . For each  $x \in G$ , the number of fixed points of  $x$  is the number of elements  $t \in S$  such that  $xt = t$ .

Since the action is transitive, for any  $t \in S$  there exists  $g \in G$  such that  $t = gs$ . Then  $xt = t$  if and only if  $xgs = gs$ , which means  $g^{-1}xg \in H$ .

Therefore,  $f(x) = \#\{g \in G : g^{-1}xg \in H\} = \#\{g \in G : x \in gHg^{-1}\}$ .

Summing over all  $x \in G$ , we get  $\sum_{x \in G} f(x) = \sum_{x \in G} \#\{g \in G : x \in gHg^{-1}\} = \sum_{g \in G} \#(gHg^{-1}) = \#(G)$ .

- (b) If  $G$  is doubly transitive, then for any two pairs  $(s_1, s_2)$  and  $(t_1, t_2)$  of distinct elements, there exists exactly one element  $g \in G$  such that  $gs_1 = t_1$  and  $gs_2 = t_2$ .

This means that for any  $x \in G$ , the number of ordered pairs  $(s, t)$  with  $s \neq t$  and  $xs = s$ ,  $xt = t$  is either 0 or 1.

Therefore,  $\sum_{x \in G} f(x)(f(x) - 1) = \#(G)$ .

Combining with part (a), we get  $\sum_{x \in G} f(x)^2 = 2\#(G)$ .

Conversely, if  $\sum_{x \in G} f(x)^2 = 2\#(G)$ , then  $\sum_{x \in G} f(x)(f(x)-1) = \#(G)$ , which means  $G$  is doubly transitive. ■

## 1.10 Fiber Products and Coproducts

### Key Definitions and Theorems:

**Definition:** A *fiber product* (or pullback) of morphisms  $f : X \rightarrow Z$  and  $g : Y \rightarrow Z$  is an object  $X \times_Z Y$  with morphisms  $p_1 : X \times_Z Y \rightarrow X$  and  $p_2 : X \times_Z Y \rightarrow Y$  such that  $f \circ p_1 = g \circ p_2$ .

**Definition:** A *fiber coproduct* (or pushout) of morphisms  $f : Z \rightarrow X$  and  $g : Z \rightarrow Y$  is an object  $X \oplus_Z Y$  with morphisms  $i_1 : X \rightarrow X \oplus_Z Y$  and  $i_2 : Y \rightarrow X \oplus_Z Y$  such that  $i_1 \circ f = i_2 \circ g$ .

**Universal Property of Fiber Product:** For any object  $W$  with morphisms  $h : W \rightarrow X$  and  $k : W \rightarrow Y$  such that  $f \circ h = g \circ k$ , there exists a unique morphism  $\phi : W \rightarrow X \times_Z Y$  such that  $p_1 \circ \phi = h$  and  $p_2 \circ \phi = k$ .

**Universal Property of Fiber Coproduct:** For any object  $W$  with morphisms  $h : X \rightarrow W$  and  $k : Y \rightarrow W$  such that  $h \circ f = k \circ g$ , there exists a unique morphism  $\phi : X \oplus_Z Y \rightarrow W$  such that  $\phi \circ i_1 = h$  and  $\phi \circ i_2 = k$ .

**Construction in Abelian Groups:** The fiber product is  $X \times_Z Y = \{(x, y) \in X \times Y : f(x) = g(y)\}$ .

**Construction in Abelian Groups:** The fiber coproduct is  $X \oplus_Z Y = (X \oplus Y)/W$  where  $W = \{(f(z), -g(z)) : z \in Z\}$ .

**Theorem:** The pullback of a surjective homomorphism is surjective.

**Theorem:** The pushout of an injective homomorphism is injective.

**Definition:** A *free product* of groups  $G$  and  $H$  is the coproduct in the category of groups.

**Definition:** An *amalgamated free product*  $G *_H G'$  is the coproduct of homomorphisms  $f : H \rightarrow G$  and  $g : H \rightarrow G'$ .

## 1.50: Fiber products in abelian groups

- (a) Show that fiber products exist in the category of abelian groups. In fact, if  $X, Y$  are abelian groups with homomorphisms  $f : X \rightarrow Z$  and  $g : Y \rightarrow Z$  show that  $X \times_Z Y$  is the set of all pairs  $(x, y)$  with  $x \in X$  and  $y \in Y$  such that  $f(x) = g(y)$ . The maps  $p_1, p_2$  are the projections on the first and second factor respectively.
- (b) Show that the pull-back of a surjective homomorphism is surjective.

**Strategy:** For part (a), verify that the given set is a subgroup and satisfies the universal property. For part (b), use the surjectivity of  $f$  to show that for any  $y \in Y$ , there exists  $x \in X$  such that  $f(x) = g(y)$ .

**Solution:**

- (a) Let  $X \times_Z Y = \{(x, y) \in X \times Y : f(x) = g(y)\}$ . This is a subgroup of  $X \times Y$  because if  $(x_1, y_1), (x_2, y_2) \in X \times_Z Y$ , then  $f(x_1) = g(y_1)$  and  $f(x_2) = g(y_2)$ , so  $f(x_1 + x_2) = f(x_1) + f(x_2) = g(y_1) + g(y_2) = g(y_1 + y_2)$ , so  $(x_1 + x_2, y_1 + y_2) \in X \times_Z Y$ .

The projections  $p_1 : X \times_Z Y \rightarrow X$  and  $p_2 : X \times_Z Y \rightarrow Y$  are homomorphisms, and  $f \circ p_1 = g \circ p_2$ .

If  $W$  is another abelian group with homomorphisms  $h : W \rightarrow X$  and  $k : W \rightarrow Y$  such that  $f \circ h = g \circ k$ , then the unique homomorphism  $\phi : W \rightarrow X \times_Z Y$  is given by  $\phi(w) = (h(w), k(w))$ .

- (b) Let  $f : X \rightarrow Z$  be surjective and let  $g : Y \rightarrow Z$  be any homomorphism. We show that  $p_2 : X \times_Z Y \rightarrow Y$  is surjective.

For any  $y \in Y$ , let  $z = g(y)$ . Since  $f$  is surjective, there exists  $x \in X$  such that  $f(x) = z = g(y)$ . Then  $(x, y) \in X \times_Z Y$  and  $p_2(x, y) = y$ .

■

## 1.51: Fiber products in sets

- (a) Show that fiber products exist in the category of sets.

- (b) In any category  $\mathcal{C}$ , consider the category  $\mathcal{C}_Z$  of objects over  $Z$ . Let  $h : T \rightarrow Z$  be a fixed object in this category. Let  $F$  be the functor such that

$$F(X) = \text{Mor}_Z(T, X),$$

where  $X$  is an object over  $Z$ , and  $\text{Mor}_Z$  denotes morphisms over  $Z$ . Show that  $F$  transforms fiber products over  $Z$  into products in the category of sets. (Actually, once you have understood the definitions, this is tautological.)

**Strategy:** For part (a), use the same construction as for abelian groups. For part (b), use the universal property of fiber products to show that morphisms from  $T$  to the fiber product correspond to pairs of morphisms from  $T$  to  $X$  and  $Y$ .

**Solution:**

- (a) Let  $X, Y$  be sets with functions  $f : X \rightarrow Z$  and  $g : Y \rightarrow Z$ . The fiber product  $X \times_Z Y = \{(x, y) \in X \times Y : f(x) = g(y)\}$  with projections  $p_1 : X \times_Z Y \rightarrow X$  and  $p_2 : X \times_Z Y \rightarrow Y$  satisfies the universal property.
- (b) The functor  $F$  sends an object  $X$  over  $Z$  to the set of morphisms from  $T$  to  $X$  over  $Z$ .

If  $X \times_Z Y$  is the fiber product of  $X$  and  $Y$  over  $Z$ , then  $F(X \times_Z Y) = \text{Mor}_Z(T, X \times_Z Y)$ .

By the universal property of the fiber product, a morphism  $T \rightarrow X \times_Z Y$  over  $Z$  is equivalent to a pair of morphisms  $T \rightarrow X$  and  $T \rightarrow Y$  over  $Z$ .

Therefore,  $F(X \times_Z Y) \cong F(X) \times F(Y)$ , which is the product in the category of sets.

■

### 1.52: Push-outs in abelian groups

- (a) Show that push-outs (i.e. fiber coproducts) exist in the category of abelian groups. In this case the fiber coproduct of two

homomorphisms  $f, g$  as above is denoted by  $X \oplus_Z Y$ . Show that it is the factor group

$$X \oplus_Z Y = (X \oplus Y)/W,$$

where  $W$  is the subgroup consisting of all elements  $(f(z), -g(z))$  with  $z \in Z$ .

- (b) Show that the push-out of an injective homomorphism is injective.

**Remark.** After you have read about modules over rings, you should note that the above two exercises apply to modules as well as to abelian groups.

**Strategy:** For part (a), verify that the given construction satisfies the universal property of push-outs. For part (b), use the injectivity of  $f$  to show that if  $(0, y) \in W$ , then  $y = 0$ .

**Solution:**

- (a) Let  $X \oplus_Z Y = (X \oplus Y)/W$  where  $W = \{(f(z), -g(z)) : z \in Z\}$ . The maps  $i_1 : X \rightarrow X \oplus_Z Y$  and  $i_2 : Y \rightarrow X \oplus_Z Y$  are given by  $i_1(x) = (x, 0) + W$  and  $i_2(y) = (0, y) + W$ .

These maps satisfy  $i_1 \circ f = i_2 \circ g$  because  $(f(z), 0) + W = (0, g(z)) + W$  for all  $z \in Z$ .

If  $A$  is another abelian group with homomorphisms  $h : X \rightarrow A$  and  $k : Y \rightarrow A$  such that  $h \circ f = k \circ g$ , then the unique homomorphism  $\phi : X \oplus_Z Y \rightarrow A$  is given by  $\phi((x, y) + W) = h(x) + k(y)$ .

- (b) Let  $f : Z \rightarrow X$  be injective and let  $g : Z \rightarrow Y$  be any homomorphism. We show that  $i_2 : Y \rightarrow X \oplus_Z Y$  is injective.

If  $i_2(y) = 0$ , then  $(0, y) \in W$ , so  $(0, y) = (f(z), -g(z))$  for some  $z \in Z$ . Since  $f$  is injective,  $z = 0$ , so  $y = -g(0) = 0$ .

■

## 1.53: Coproduct of homomorphisms

Let  $H, G, G'$  be groups, and let

$$f : H \rightarrow G, \quad g : H \rightarrow G'$$

be two homomorphisms. Define the notion of coproduct of these two homomorphisms over  $H$ , and show that it exists.

**Strategy:** Define the coproduct using the universal property and show that it exists as the amalgamated free product  $G *_H G'$ , which is the quotient of the free product by the normal subgroup generated by relations  $f(h) = g(h)$  for all  $h \in H$ .

**Solution:** The coproduct of the homomorphisms  $f : H \rightarrow G$  and  $g : H \rightarrow G'$  over  $H$  is a group  $K$  with homomorphisms  $i_1 : G \rightarrow K$  and  $i_2 : G' \rightarrow K$  such that  $i_1 \circ f = i_2 \circ g$ , and for any group  $L$  with homomorphisms  $h : G \rightarrow L$  and  $k : G' \rightarrow L$  satisfying  $h \circ f = k \circ g$ , there exists a unique homomorphism  $\phi : K \rightarrow L$  such that  $\phi \circ i_1 = h$  and  $\phi \circ i_2 = k$ .

This coproduct exists and is given by the amalgamated free product  $G *_H G'$ . This is the quotient of the free product  $G * G'$  by the normal subgroup generated by all elements of the form  $f(h)g(h)^{-1}$  for  $h \in H$ .

The maps  $i_1$  and  $i_2$  are the natural inclusions of  $G$  and  $G'$  into the free product, followed by the quotient map. ■

## 1.54: Tits' coproduct criterion

Let  $G$  be a group and let  $\{G_i\}_{i \in I}$  be a family of subgroups generating  $G$ . Suppose  $G$  operates on a set  $S$ . For each  $i \in I$ , suppose given a subset  $S_i$  of  $S$ , and let  $s$  be a point of  $S - \bigcup_S S_i$ . Assume that for each  $g \in G_i - \{e\}$ , we have

$$gS_j \subset S_i \text{ for all } j \neq i, \quad \text{and } g(s) \in S_i \text{ for all } i.$$

Prove that  $G$  is the coproduct of the family  $\{G_i\}_{i \in I}$ . (Hint: Suppose a product  $g_1 \cdots g_m = id$  on  $S$ . Apply this product to  $s$ , and use Proposition 12.4.)

**Strategy:** Show that any non-trivial reduced word in the  $G_i$  acts non-trivially on  $S$  by induction on the length of the word. Use the given conditions to show that the action moves the point  $s$  to a specific subset.

**Solution:** We show that any non-trivial reduced word in the  $G_i$  acts non-trivially on  $S$ , which implies that  $G$  is the coproduct of the  $G_i$ .

Let  $g_1 \cdots g_m$  be a reduced word where  $g_k \in G_{i_k}$  and  $i_k \neq i_{k+1}$  for all  $k$ .

We show by induction on  $m$  that  $g_1 \cdots g_m(s) \in S_{i_1}$ .

For  $m = 1$ , this follows from the assumption that  $g_1(s) \in S_{i_1}$ .

For  $m > 1$ , let  $s' = g_2 \cdots g_m(s)$ . By induction,  $s' \in S_{i_2}$ . Since  $g_1 \in G_{i_1}$  and  $i_1 \neq i_2$ , we have  $g_1(s') \in S_{i_1}$  by the assumption that  $g_1 S_j \subset S_{i_1}$  for all  $j \neq i_1$ .

Therefore,  $g_1 \cdots g_m(s) = g_1(s') \in S_{i_1} \neq \{s\}$ , so  $g_1 \cdots g_m \neq id$ .

This shows that  $G$  is the coproduct of the  $G_i$ . ■

### 1.55: Fixed points of Möbius transformations

Let  $M \in GL_2(\mathbb{C})$  ( $2 \times 2$  complex matrices with non-zero determinant). We let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ and for } z \in \mathbb{C} \text{ we let } M(z) = \frac{az + b}{cz + d}.$$

If  $z = -d/c$  ( $c \neq 0$ ) then we put  $M(z) = \infty$ . Then you can verify (and you should have seen something like this in a course in complex analysis) that  $GL_2(\mathbb{C})$  thus operates on  $\mathbb{C} \cup \{\infty\}$ . Let  $\lambda, \lambda'$  be the eigenvalues of  $M$  viewed as a linear map on  $\mathbb{C}^2$ . Let  $W, W'$  be the corresponding eigenvectors,

$$W = ' (w_1, w_2) \text{ and } W' = ' (w'_1, w'_2).$$

By a fixed point of  $M$  on  $\mathbb{C}$  we mean a complex number  $z$  such that  $M(z) = z$ . Assume that  $M$  has two distinct fixed points  $\neq \infty$ .

- (a) Show that there cannot be more than two fixed points and that these fixed points are  $w = w_1/w_2$  and  $w' = w'_1/w'_2$ . In fact one may take

$$W = ' (w, 1), W' = ' (w', 1).$$

- (b) Assume that  $|\lambda| < |\lambda'|$ . Given  $z \neq w$ , show that

$$\lim_{k \rightarrow \infty} M^k(z) = w'.$$



[Hint: Let  $S = (W, W')$  and consider  $S^{-1}M^kS(z) = \alpha^k z$  where  $\alpha = \lambda/\lambda'$ .]

**Strategy:** For part (a), solve the fixed point equation and show it's quadratic. For part (b), diagonalize the matrix using eigenvectors and use the fact that  $|\alpha| < 1$  to show convergence.

**Solution:**

- (a) The fixed points of  $M$  are the solutions to  $M(z) = z$ , which gives the equation  $cz^2 + (d-a)z - b = 0$ . This is a quadratic equation, so there are at most two fixed points.

If  $W = (w_1, w_2)$  is an eigenvector with eigenvalue  $\lambda$ , then  $MW = \lambda W$ , so  $aw_1 + bw_2 = \lambda w_1$  and  $cw_1 + dw_2 = \lambda w_2$ .

This gives  $w_1/w_2 = (b)/(\lambda-a) = (\lambda-d)/c$ . If we take  $W = (w, 1)$  where  $w = w_1/w_2$ , then  $w$  satisfies the fixed point equation.

- (b) Let  $S = (W, W')$  be the matrix with columns  $W$  and  $W'$ . Then
- $$S^{-1}MS = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix}.$$

For any  $z \in \mathbb{C}$ , we have  $S^{-1}M^kS(z) = \alpha^k z$  where  $\alpha = \lambda/\lambda'$ .

Since  $|\alpha| < 1$ , we have  $\lim_{k \rightarrow \infty} \alpha^k = 0$ , so  $\lim_{k \rightarrow \infty} S^{-1}M^kS(z) = 0$ .

This means  $\lim_{k \rightarrow \infty} M^k(z) = S(0) = w'$ .

■

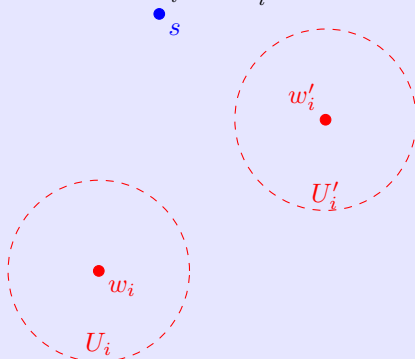
### 1.56: Free subgroup of $GL_2(\mathbb{C})$

Let  $M_1, \dots, M_r \in GL_2(\mathbb{C})$  be a finite number of matrices. Let  $\lambda_i, \lambda_j$  be the eigenvalues of  $M_i$ . Assume that each  $M_i$  has two distinct complex fixed points, and that  $|\lambda_i| < |\lambda_j|$ . Also assume that the fixed points for  $M_1, \dots, M_r$  are all distinct from each other. Prove that there exists a positive integer  $k$  such that  $M_1^k, \dots, M_r^k$  are the free generators of a free subgroup of  $GL_2(\mathbb{C})$ . [Hint: Let  $w_i, w'_i$  be the fixed points of  $M_i$ . Let  $U_i$  be a small disc centered at  $w_i$  and  $U'_i$  a small disc centered at  $w'_i$ . Let  $S_i = U_i \cup U'_i$ . Let  $s$  be a complex

number which does not lie in any  $S_i$ . Let  $G_i = \langle M_i^k \rangle$ . Show that the conditions of Exercise 54 are satisfied for  $k$  sufficiently large.]

**Strategy:** Use the hint to construct neighborhoods around fixed points and show that for large enough  $k$ , the action of  $M_i^k$  satisfies the conditions of Exercise 54, which guarantees that the group is a free product.

**Solution:** Let  $w_i, w'_i$  be the fixed points of  $M_i$  with  $|w_i| < |w'_i|$ . Let  $U_i$  be a small disc centered at  $w_i$  and  $U'_i$  a small disc centered at  $w'_i$ .



Let  $S_i = U_i \cup U'_i$ .

**Solution:** Let  $w_i, w'_i$  be the fixed points of  $M_i$  with  $|w_i| < |w'_i|$ . Let  $U_i$  be a small disc centered at  $w_i$  and  $U'_i$  a small disc centered at  $w'_i$ . Let  $S_i = U_i \cup U'_i$ .

Let  $s$  be a complex number not in any  $S_i$ . For  $k$  sufficiently large, the action of  $M_i^k$  on  $\mathbb{C} \cup \{\infty\}$  satisfies the conditions of Exercise 54:

1. For any  $g \in \langle M_i^k \rangle - \{e\}$ , we have  $gS_j \subset S_i$  for all  $j \neq i$  because  $M_i^k$  contracts towards the fixed points of  $M_i$ .
2. For any  $g \in \langle M_i^k \rangle - \{e\}$ , we have  $g(s) \in S_i$  because  $M_i^k$  maps points outside  $S_i$  into  $S_i$  for large enough  $k$ .

Therefore, by Exercise 54, the group generated by  $M_1^k, \dots, M_r^k$  is the free product of the cyclic groups  $\langle M_i^k \rangle$ .

■

### 1.57: Group generated by stabilizers

Let  $G$  be a group acting on a set  $X$ . Let  $Y$  be a subset of  $X$ . Let  $G_Y$  be the subset of  $G$  consisting of those elements  $g$  such that  $gY \cap Y$

is not empty. Let  $\overline{G}_Y$  be the subgroup of  $G$  generated by  $G_Y$ . Then  $\overline{G}_Y Y$  and  $(G - \overline{G}_Y)Y$  are disjoint. [Hint: Suppose that there exist  $g_1 \in \overline{G}_Y$  and  $g_2 \in G$  but  $g_2 \notin \overline{G}_Y$ , and elements  $y_1, y_2 \in Y$  such that  $g_2 y_1 = g_1 y_2$ . Then  $g_2^{-1} g_1 y_1 = y_2$ , so  $g_2^{-1} g_1 \in G_Y$  whence  $g_2 \in \overline{G}_Y$ , contrary to assumption.]

Application. Suppose that  $X = GY$ , but that  $X$  cannot be expressed as a disjoint union as above unless one of the two sets is empty. Then we conclude that  $G - \overline{G}_Y$  is empty, and therefore  $G_Y$  generates  $G$ .

Example 1. Suppose  $X$  is a connected topological space,  $Y$  is open, and  $G$  acts continuously. Then all translates of  $Y$  are open, so  $G$  is generated by  $G_Y$ .

Example 2. Suppose  $G$  is a discrete group acting continuously and discretely on  $X$ . Again suppose  $X$  connected and  $Y$  closed, and that any union of translates of  $Y$  by elements of  $G$  is closed, so again  $G - \overline{G}_Y$  is empty, and  $G_Y$  generates  $G$ .

**Strategy:** Use the hint to prove by contradiction. If the sets are not disjoint, then there exist elements as described in the hint, which leads to a contradiction since  $g_2^{-1} g_1 \in G_Y$  implies  $g_2 \in \overline{G}_Y$ .

**Solution:** We prove that  $\overline{G}_Y Y$  and  $(G - \overline{G}_Y)Y$  are disjoint.

Suppose for contradiction that there exist  $g_1 \in \overline{G}_Y$ ,  $g_2 \in G - \overline{G}_Y$ , and  $y_1, y_2 \in Y$  such that  $g_1 y_1 = g_2 y_2$ .

Then  $g_2^{-1} g_1 y_1 = y_2 \in Y$ , so  $g_2^{-1} g_1 \in G_Y$ . Since  $G_Y \subseteq \overline{G}_Y$ , we have  $g_2^{-1} g_1 \in \overline{G}_Y$ .

Since  $g_1 \in \overline{G}_Y$ , this implies  $g_2 \in \overline{G}_Y$ , contradicting the assumption that  $g_2 \notin \overline{G}_Y$ .

Therefore,  $\overline{G}_Y Y$  and  $(G - \overline{G}_Y)Y$  are disjoint.

**Application:** If  $X = GY$  and  $X$  cannot be expressed as a disjoint union of the form above unless one set is empty, then we must have  $G - \overline{G}_Y = \emptyset$ , which means  $G = \overline{G}_Y$ . Therefore,  $G_Y$  generates  $G$ .

**Example 1:** If  $X$  is connected and  $Y$  is open, then  $GY$  is open and connected. If  $G_Y$  did not generate  $G$ , then  $\overline{G}_Y Y$  and  $(G - \overline{G}_Y)Y$  would be disjoint open sets whose union is  $X$ , contradicting connectedness.

**Example 2:** If  $X$  is connected and  $Y$  is closed, and if  $G_Y$  did not generate  $G$ , then  $\overline{G}_Y Y$  and  $(G - \overline{G}_Y)Y$  would be disjoint closed sets whose union is  $X$ , contradicting connectedness.

## 1.11 Problem-Solving Techniques

This chapter covers fundamental group theory concepts and provides various techniques for solving group theory problems. Here is a summary of the key problem-solving strategies:

### Proving Groups are Abelian

- Use Lagrange's theorem to determine possible element orders
- Show that if  $G/Z(G)$  is cyclic, then  $G$  is abelian
- Use the fact that groups of prime order are cyclic and hence abelian
- Show that all elements commute by expressing them in terms of generators and central elements

### Classifying Groups of Small Order

1. Use Lagrange's theorem to determine possible element orders
2. Check if the group has an element of maximum possible order (making it cyclic)
3. If not, construct explicit isomorphisms to known groups
4. Use the fact that groups of order  $p^2$  are abelian and either cyclic or isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_p$

### Working with Normal Subgroups

- Show that conjugates of generators are in the subgroup
- Use the fact that normal subgroups are unions of conjugacy classes
- For commutator subgroups, show that conjugates of commutators are commutators
- Use the universal property of quotient groups for factorization properties

## Counting Arguments

1. Define a surjective map and count preimages
2. Use the inclusion-exclusion principle for unions of sets
3. Apply the orbit-stabilizer theorem:  $|G \cdot s| = (G : G_s)$
4. Use Burnside's lemma: number of orbits =  $\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$

## Sylow Theory Applications

- Use Sylow's theorems to count Sylow subgroups
- Show that if  $n_p = 1$ , then the Sylow subgroup is normal
- Use the fact that normal Sylow subgroups have trivial intersection with other Sylow subgroups
- Apply the fact that extensions of solvable groups by solvable groups are solvable

## Group Actions

1. Define an action and use it to create homomorphisms
2. Use transitivity to simplify problems (assume one element is fixed)
3. Show primitivity by proving stabilizers are maximal subgroups
4. Use double transitivity to count fixed points and derive formulas

## Permutation Groups

- Use cycle structure to determine conjugacy classes
- Show that conjugates of cycles are cycles with permuted elements
- Use the fact that  $S_n$  is generated by transpositions
- Apply the fact that  $A_n$  is  $(n - 2)$ -transitive for  $n \geq 3$

## Abelian Groups

1. Use the fundamental theorem of finite abelian groups
2. Decompose into direct products of cyclic groups of prime power orders
3. Use the structure theorem for finitely generated abelian groups
4. Apply isomorphism theorems to relate indices and quotients

## Universal Properties

- Define objects using universal properties (fiber products, push-outs)
- Show existence by constructing explicit examples
- Use universal properties to prove uniqueness
- Apply functorial properties to transform problems

## Free Products and Coproducts

1. Use Tits' criterion to show a group is a free product
2. Show that reduced words act non-trivially on some set
3. Use the universal property of free products
4. Apply the fact that free products have no non-trivial relations

## Geometric Methods

- Use geometric interpretations (dihedral groups as symmetries of polygons)
- Apply Möbius transformations and fixed point analysis
- Use complex analysis techniques for matrix groups
- Apply topological methods for group actions on connected spaces

## Proof by Contradiction

1. Assume the opposite of what you want to prove
2. Use the assumption to derive a contradiction
3. Often used with counting arguments or geometric properties
4. Particularly useful for showing uniqueness or non-existence

## Induction

- Use induction on group order for classification problems
- Induct on the length of words in free products
- Use induction on the number of generators
- Apply induction on the complexity of group structures

These techniques provide a comprehensive toolkit for approaching group theory problems, from basic classification to advanced structural analysis.

# Chapter 2

## Rings

### 2.1 Localization and Prime Ideals

**Definitions and Theorems:**

- A **multiplicative subset** of a ring  $A$  is a subset  $S$  such that  $1 \in S$  and if  $s, t \in S$  then  $st \in S$ .
- The **localization**  $S^{-1}A$  is the ring of fractions  $a/s$  where  $a \in A$  and  $s \in S$ , with the usual addition and multiplication.
- A **local ring** is a commutative ring with exactly one maximal ideal.
- A **prime ideal**  $\mathfrak{p}$  is an ideal such that if  $ab \in \mathfrak{p}$  then either  $a \in \mathfrak{p}$  or  $b \in \mathfrak{p}$ .
- A **maximal ideal** is an ideal that is maximal with respect to inclusion among proper ideals.

We let  $A$  denote a commutative ring.

#### 2.1: Maximal Ideal in Localization

Suppose that  $1 \neq 0$  in  $A$ . Let  $S$  be a multiplicative subset of  $A$  not containing 0. Let  $\mathfrak{p}$  be a maximal element in the set of ideals of  $A$  whose intersection with  $S$  is empty. Show that  $\mathfrak{p}$  is prime.



**Strategy:** Use proof by contradiction. Assume  $\mathfrak{p}$  is not prime, so there exist  $a, b \in A$  with  $ab \in \mathfrak{p}$  but  $a, b \notin \mathfrak{p}$ . Use the maximality of  $\mathfrak{p}$  to show that  $\mathfrak{p} + (a)$  and  $\mathfrak{p} + (b)$  must intersect  $S$ , then multiply the resulting equations to reach a contradiction.

**Solution:** Let  $\mathfrak{p}$  be a maximal element in the set of ideals of  $A$  whose intersection with  $S$  is empty. We need to show that  $\mathfrak{p}$  is prime.

Suppose for contradiction that  $\mathfrak{p}$  is not prime. Then there exist elements  $a, b \in A$  such that  $ab \in \mathfrak{p}$  but  $a \notin \mathfrak{p}$  and  $b \notin \mathfrak{p}$ .

Since  $a \notin \mathfrak{p}$ , the ideal  $\mathfrak{p} + (a)$  properly contains  $\mathfrak{p}$ . By maximality of  $\mathfrak{p}$ , we must have  $(\mathfrak{p} + (a)) \cap S \neq \emptyset$ . Similarly,  $(\mathfrak{p} + (b)) \cap S \neq \emptyset$ .

This means there exist  $p_1, p_2 \in \mathfrak{p}$ ,  $r_1, r_2 \in A$ , and  $s_1, s_2 \in S$  such that:

$$p_1 + r_1a = s_1 \quad \text{and} \quad p_2 + r_2b = s_2$$

Multiplying these equations:

$$(p_1 + r_1a)(p_2 + r_2b) = s_1s_2$$

Expanding the left side:

$$p_1p_2 + p_1r_2b + p_2r_1a + r_1r_2ab = s_1s_2$$

Since  $p_1, p_2, ab \in \mathfrak{p}$ , we have  $p_1p_2 + p_1r_2b + p_2r_1a + r_1r_2ab \in \mathfrak{p}$ . But  $s_1s_2 \in S$  since  $S$  is multiplicative. This contradicts the fact that  $\mathfrak{p} \cap S = \emptyset$ .

Therefore,  $\mathfrak{p}$  must be prime. ■

## 2.2: Surjective Homomorphism Preserves Local Property

Let  $f : A \rightarrow A'$  be a surjective homomorphism of rings, and assume that  $A$  is local,  $A' \neq 0$ . Show that  $A'$  is local.

**Strategy:** Show that  $f(\mathfrak{m})$  is the unique maximal ideal of  $A'$ , where  $\mathfrak{m}$  is the unique maximal ideal of  $A$ . Use the surjectivity of  $f$  and the correspondence between ideals to establish both maximality and uniqueness.

**Solution:** Let  $\mathfrak{m}$  be the unique maximal ideal of  $A$ . Since  $f$  is surjective,  $f(\mathfrak{m})$  is an ideal of  $A'$ .

We claim that  $f(\mathfrak{m})$  is the unique maximal ideal of  $A'$ .

First,  $f(\mathfrak{m})$  is maximal: if  $I$  is an ideal of  $A'$  containing  $f(\mathfrak{m})$ , then  $f^{-1}(I)$  is an ideal of  $A$  containing  $\mathfrak{m}$ . Since  $\mathfrak{m}$  is maximal, either

$f^{-1}(I) = \mathfrak{m}$  or  $f^{-1}(I) = A$ . If  $f^{-1}(I) = A$ , then  $I = A'$  since  $f$  is surjective. If  $f^{-1}(I) = \mathfrak{m}$ , then  $I = f(\mathfrak{m})$ . Thus  $f(\mathfrak{m})$  is maximal.

Second,  $f(\mathfrak{m})$  is unique: if  $I$  is any maximal ideal of  $A'$ , then  $f^{-1}(I)$  is a proper ideal of  $A$  (since  $f$  is surjective and  $A' \neq 0$ ). Since  $\mathfrak{m}$  is the unique maximal ideal,  $f^{-1}(I) \subseteq \mathfrak{m}$ , which implies  $I \subseteq f(\mathfrak{m})$ . By maximality of  $I$ , we have  $I = f(\mathfrak{m})$ .

Therefore,  $A'$  has exactly one maximal ideal and is local. ■

### 2.3: Unique Maximal Ideal in Localization

Let  $\mathfrak{p}$  be a prime ideal of  $A$ . Show that  $A_{\mathfrak{p}}$  has a unique maximal ideal, consisting of all elements  $a/s$  with  $a \in \mathfrak{p}$  and  $s \notin \mathfrak{p}$ .

**Strategy:** Define  $\mathfrak{m} = \{a/s : a \in \mathfrak{p}, s \notin \mathfrak{p}\}$  and show it is the unique maximal ideal by proving it's an ideal, maximal (every element not in it is a unit), and unique (any proper ideal is contained in it).

**Solution:** Let  $S = A \setminus \mathfrak{p}$ . Since  $\mathfrak{p}$  is prime,  $S$  is a multiplicative subset of  $A$ .

Let  $\mathfrak{m} = \{a/s : a \in \mathfrak{p}, s \notin \mathfrak{p}\}$ . We need to show that  $\mathfrak{m}$  is the unique maximal ideal of  $A_{\mathfrak{p}}$ .

First,  $\mathfrak{m}$  is an ideal: if  $a_1/s_1, a_2/s_2 \in \mathfrak{m}$ , then  $a_1/s_1 + a_2/s_2 = (a_1s_2 + a_2s_1)/(s_1s_2) \in \mathfrak{m}$  since  $a_1s_2 + a_2s_1 \in \mathfrak{p}$  and  $s_1s_2 \notin \mathfrak{p}$ . If  $a/s \in \mathfrak{m}$  and  $b/t \in A_{\mathfrak{p}}$ , then  $(a/s)(b/t) = (ab)/(st) \in \mathfrak{m}$  since  $ab \in \mathfrak{p}$  and  $st \notin \mathfrak{p}$ .

Second,  $\mathfrak{m}$  is maximal: if  $a/s \in A_{\mathfrak{p}} \setminus \mathfrak{m}$ , then  $a \notin \mathfrak{p}$ , so  $a \in S$ . Then  $s/a \in A_{\mathfrak{p}}$  and  $(a/s)(s/a) = 1$ , so  $a/s$  is a unit. This shows that every element not in  $\mathfrak{m}$  is a unit, which means  $\mathfrak{m}$  is maximal.

Finally,  $\mathfrak{m}$  is unique: any proper ideal  $I$  of  $A_{\mathfrak{p}}$  must be contained in  $\mathfrak{m}$ , since if  $I$  contains an element  $a/s$  with  $a \notin \mathfrak{p}$ , then  $a/s$  is a unit, which would make  $I = A_{\mathfrak{p}}$ .

Therefore,  $A_{\mathfrak{p}}$  is a local ring with unique maximal ideal  $\mathfrak{m}$ . ■

## 2.2 Principal and Factorial Rings

### Definitions and Theorems:

- A **principal ring** (PID) is an integral domain in which every ideal is principal (generated by a single element).

- A **factorial ring** (UFD) is an integral domain in which every non-zero non-unit element can be written as a product of irreducible elements, and this factorization is unique up to order and units.
- A **prime element**  $p$  in a ring  $A$  is a non-zero non-unit such that if  $p$  divides  $ab$  then  $p$  divides  $a$  or  $p$  divides  $b$ .
- An **irreducible element**  $p$  is a non-zero non-unit such that if  $p = ab$  then either  $a$  or  $b$  is a unit.
- A **greatest common divisor** (GCD) of elements  $a_1, \dots, a_n$  is an element  $d$  such that  $d$  divides each  $a_i$  and if  $e$  divides each  $a_i$  then  $e$  divides  $d$ .

#### 2.4: Localization Preserves Principal Property

Let  $A$  be a principal ring and  $S$  a multiplicative subset with  $0 \notin S$ . Show that  $S^{-1}A$  is principal.

**Strategy:** For any ideal  $I$  of  $S^{-1}A$ , consider the ideal  $J = \{a \in A : a/1 \in I\}$  of  $A$ . Since  $A$  is principal,  $J = (d)$  for some  $d \in A$ . Show that  $I = (d/1)$ .

**Solution:** Let  $I$  be an ideal of  $S^{-1}A$ . We need to show that  $I$  is principal.

Let  $J = \{a \in A : a/1 \in I\}$ . Then  $J$  is an ideal of  $A$ . Since  $A$  is principal,  $J = (d)$  for some  $d \in A$ .

We claim that  $I = (d/1)$ .

First, if  $a/1 \in I$ , then  $a \in J = (d)$ , so  $a = rd$  for some  $r \in A$ . Then  $a/1 = (rd)/1 = (r/1)(d/1) \in (d/1)$ .

Second, if  $a/s \in I$ , then  $a/1 = (a/s)(s/1) \in I$ , so  $a \in J = (d)$ . Thus  $a = rd$  for some  $r \in A$ , and  $a/s = (rd)/s = (r/s)(d/1) \in (d/1)$ .

Therefore,  $I = (d/1)$  and  $S^{-1}A$  is principal. ■

#### 2.5: Localization Preserves Factorial Property

Let  $A$  be a factorial ring and  $S$  a multiplicative subset with  $0 \notin S$ . Show that  $S^{-1}A$  is factorial, and that the prime elements of  $S^{-1}A$

are of the form  $up$  with primes  $p$  of  $A$  such that  $(p) \cap S$  is empty, and units  $u$  in  $S^{-1}A$ .

**Strategy:** Use the factorization of elements in  $A$  to show that  $S^{-1}A$  is factorial. For the prime elements, show that elements in  $S$  become units in  $S^{-1}A$ , while irreducible elements not in  $S$  remain irreducible, and use the unique factorization property of  $A$ .

**Solution:** First, we show that  $S^{-1}A$  is factorial. Let  $a/s \in S^{-1}A$  be a non-zero non-unit. Then  $a \in A$  is non-zero and not a unit in  $S^{-1}A$ .

Since  $A$  is factorial,  $a$  can be written as a product of irreducible elements in  $A$ :  $a = p_1 \cdots p_n$ . Then  $a/s = (p_1/1) \cdots (p_n/1)(1/s)$ .

We need to show that each  $p_i/1$  is either irreducible or a unit in  $S^{-1}A$ . If  $p_i \in S$ , then  $p_i/1$  is a unit. If  $p_i \notin S$ , then  $p_i/1$  is irreducible in  $S^{-1}A$  (since if  $p_i/1 = (a/s)(b/t)$ , then  $p_i st = ab$ , which would contradict the irreducibility of  $p_i$  in  $A$  unless one of  $a$  or  $b$  is a unit).

For uniqueness, suppose  $a/s = (p_1/1) \cdots (p_m/1)(1/s_1) = (q_1/1) \cdots (q_n/1)(1/s_2)$  where  $p_i, q_j$  are irreducible in  $A$  and not in  $S$ . Then  $as_1 = p_1 \cdots p_m$  and  $as_2 = q_1 \cdots q_n$ . Since  $A$  is factorial, these factorizations are the same up to units and order.

For the second part, let  $p$  be a prime element of  $A$  such that  $(p) \cap S = \emptyset$ . We show that  $p/1$  is prime in  $S^{-1}A$ . If  $(p/1)$  divides  $(a/s)(b/t)$ , then  $p$  divides  $ab$  in  $A$ , so  $p$  divides  $a$  or  $p$  divides  $b$ . Thus  $(p/1)$  divides  $(a/s)$  or  $(b/t)$ .

Conversely, if  $q$  is a prime element of  $S^{-1}A$ , then  $q = a/s$  where  $a \in A$  is irreducible and  $a \notin S$ . Since  $q$  is prime,  $a$  must be prime in  $A$ . ■

## 2.6: Localization at Prime is Principal

Let  $A$  be a factorial ring and  $p$  a prime element. Show that the local ring  $A_{(p)}$  is principal.

**Strategy:** Use Problem 2.4 since factorial rings are principal, or show directly that any ideal  $I$  of  $A_{(p)}$  corresponds to an ideal  $J$  of  $A$  contained in  $(p)$ , which must be  $(p^n)$  for some  $n \geq 0$ .

**Solution:** Let  $S = A \setminus (p)$ . Then  $A_{(p)} = S^{-1}A$ .

By Problem 2.4, since  $A$  is principal (factorial rings are principal),  $A_{(p)}$  is principal.

Alternatively, we can show this directly. Let  $I$  be an ideal of  $A_{(p)}$ . Let  $J = \{a \in A : a/1 \in I\}$ . Then  $J$  is an ideal of  $A$  contained in  $(p)$  (since if  $a \notin (p)$ , then  $a/1$  is a unit in  $A_{(p)}$ ).

Since  $A$  is factorial,  $J = (p^n)$  for some  $n \geq 0$ . Then  $I = (p^n/1) = (p/1)^n$ . ■

### 2.7: GCD in Principal Rings

Let  $A$  be a principal ring and  $a_1, \dots, a_n$  non-zero elements of  $A$ . Let  $(a_1, \dots, a_n) = (d)$ . Show that  $d$  is a greatest common divisor for the  $a_i$  ( $i = 1, \dots, n$ ).

**Strategy:** Show that  $d$  divides each  $a_i$  (since  $(a_1, \dots, a_n) \subseteq (d)$ ), and that any common divisor  $e$  of the  $a_i$  divides  $d$  (using the fact that  $d$  is a linear combination of the  $a_i$ ).

**Solution:** Since  $(a_1, \dots, a_n) = (d)$ , we have  $d \in (a_1, \dots, a_n)$ , so  $d = r_1 a_1 + \dots + r_n a_n$  for some  $r_i \in A$ . This shows that  $d$  is a linear combination of the  $a_i$ .

Also, since  $(a_1, \dots, a_n) \subseteq (d)$ , each  $a_i \in (d)$ , so  $d$  divides each  $a_i$ .

Now let  $e$  be any element that divides each  $a_i$ . Then  $a_i = s_i e$  for some  $s_i \in A$ . Since  $d = r_1 a_1 + \dots + r_n a_n = r_1 (s_1 e) + \dots + r_n (s_n e) = (r_1 s_1 + \dots + r_n s_n) e$ , we have  $e$  divides  $d$ .

Therefore,  $d$  is a greatest common divisor of the  $a_i$ . ■

## 2.3 Group of Units

### Definitions and Theorems:

- The **group of units** of a ring  $A$  is the set of all invertible elements, denoted  $A^*$ .
- A **cyclic group** is a group generated by a single element.
- A group is of **type**  $(n_1, n_2, \dots, n_k)$  if it is isomorphic to  $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ .
- The **Euler totient function**  $\phi(n)$  counts the number of integers between 1 and  $n$  that are coprime to  $n$ .

### 2.8: Structure of Units Modulo $p^r$

Let  $p$  be a prime number, and let  $A$  be the ring  $\mathbb{Z}/p^r\mathbb{Z}$  ( $r = \text{integer} \geq 1$ ). Let  $G$  be the group of units in  $A$ , i.e. the group of integers prime to  $p$ , modulo  $p^r$ . Show that  $G$  is cyclic, except in the case when

$$p = 2, \quad r \geq 3,$$

in which case it is of type  $(2, 2^{r-2})$ .

[Hint: In the general case, show that  $G$  is the product of a cyclic group generated by  $1 + p$ , and a cyclic group of order  $p - 1$ . In the exceptional case, show that  $G$  is the product of the group  $\{\pm 1\}$  with the cyclic group generated by the residue class of 5 mod  $2^r$ .]

**Strategy:** Use induction on  $r$  and the structure of the multiplicative group modulo prime powers. For odd primes, use the exact sequence involving  $U_1$  and  $(\mathbb{Z}/p\mathbb{Z})^*$ . For  $p = 2$ , handle the exceptional case by showing that  $G$  is the product of  $\{\pm 1\}$  and a cyclic group generated by 5.

**Solution:** We will prove this by induction on  $r$ . The key insight is to use the structure of the multiplicative group modulo prime powers.

For  $r = 1$ ,  $G = (\mathbb{Z}/p\mathbb{Z})^*$  is cyclic of order  $p - 1$  by the primitive root theorem.

For  $r > 1$ , we consider the exact sequence:

$$1 \rightarrow U_1 \rightarrow G \rightarrow (\mathbb{Z}/p\mathbb{Z})^* \rightarrow 1$$

where  $U_1 = \{1 + ap : a \in \mathbb{Z}/p^{r-1}\mathbb{Z}\}$ .

The group  $U_1$  is isomorphic to the additive group  $\mathbb{Z}/p^{r-1}\mathbb{Z}$  via the map  $1 + ap \mapsto a$ . This is a cyclic group of order  $p^{r-1}$ .

For odd primes  $p$ ,  $U_1$  is cyclic and  $(\mathbb{Z}/p\mathbb{Z})^*$  is cyclic of order  $p - 1$ . Since  $\gcd(p^{r-1}, p - 1) = 1$ , the group  $G$  is cyclic.

For  $p = 2$ , we need to be more careful. For  $r = 2$ ,  $G$  is cyclic of order 1. For  $r = 3$ ,  $G$  has order 2 and is cyclic.

For  $r \geq 3$ , the group  $U_1$  is cyclic of order  $2^{r-1}$ , but  $(\mathbb{Z}/2\mathbb{Z})^*$  is trivial. However, the group  $U_2 = \{1 + 4a : a \in \mathbb{Z}/2^{r-2}\mathbb{Z}\}$  is cyclic of order  $2^{r-2}$ .

The group  $G$  is the product of  $\{\pm 1\}$  (which has order 2) and the cyclic group generated by 5 (which has order  $2^{r-2}$ ). Since these groups have coprime orders,  $G$  is of type  $(2, 2^{r-2})$ .

The key fact is that 5 generates a cyclic subgroup of order  $2^{r-2}$  in  $G$  for  $r \geq 3$ , and this subgroup together with  $\{\pm 1\}$  generates all of  $G$ . ■

## 2.4 Quadratic Rings

### Definitions and Theorems:

- A **quadratic ring** is a subring of  $\mathbb{C}$  of the form  $\mathbb{Z}[\sqrt{d}]$  where  $d$  is a square-free integer.
- The **norm** of an element  $a + b\sqrt{d}$  is  $N(a + b\sqrt{d}) = a^2 - db^2$ .
- A **unit** in a ring is an element with a multiplicative inverse.
- An **irreducible element** is a non-zero non-unit that cannot be written as a product of two non-units.
- The **Gaussian integers** are the ring  $\mathbb{Z}[i]$  where  $i = \sqrt{-1}$ .

### 2.9: Principal Ring of Gaussian Integers

Let  $i$  be the complex number  $\sqrt{-1}$ . Show that the ring  $\mathbb{Z}[i]$  is principal, and hence factorial. What are the units?

**Strategy:** Use the Euclidean algorithm with the norm function  $N(a + bi) = a^2 + b^2$ . For any ideal  $I$ , choose an element  $\alpha$  with minimal norm and show that  $I = (\alpha)$  by using the division algorithm in  $\mathbb{C}$  and the fact that the norm decreases in each step.

**Solution:** To show that  $\mathbb{Z}[i]$  is principal, we use the Euclidean algorithm with the norm function  $N(a + bi) = a^2 + b^2$ .

Let  $I$  be a non-zero ideal of  $\mathbb{Z}[i]$ . Let  $\alpha$  be a non-zero element of  $I$  with minimal norm. We claim that  $I = (\alpha)$ .

Let  $\beta \in I$ . We need to show that  $\alpha$  divides  $\beta$ . Consider the complex number  $\beta/\alpha = x + yi$  where  $x, y \in \mathbb{Q}$ . Let  $m, n$  be integers such that  $|x - m| \leq 1/2$  and  $|y - n| \leq 1/2$ .

Let  $\gamma = \beta - \alpha(m + ni)$ . Then  $\gamma \in I$  and  $N(\gamma) = N(\alpha)N((x - m) + (y - n)i) = N(\alpha)((x - m)^2 + (y - n)^2) < N(\alpha)$  since  $(x - m)^2 + (y - n)^2 \leq 1/4 + 1/4 = 1/2 < 1$ .

By minimality of  $N(\alpha)$ , we must have  $\gamma = 0$ , so  $\beta = \alpha(m + ni)$ . Therefore,  $I = (\alpha)$ .

Since  $\mathbb{Z}[i]$  is principal, it is also factorial (UFD).

The units of  $\mathbb{Z}[i]$  are the elements with norm 1. These are  $\pm 1, \pm i$ . ■

### 2.10: Non-Factorial Quadratic Ring

Let  $D$  be an integer  $\geq 1$ , and let  $R$  be the set of all elements  $a+b\sqrt{-D}$  with  $a, b \in \mathbb{Z}$ .

- Show that  $R$  is a ring.
- Using the fact that complex conjugation is an automorphism of  $\mathbb{C}$ , show that complex conjugation induces an automorphism of  $R$ .
- Show that if  $D \geq 2$  then the only units in  $R$  are  $\pm 1$ .
- Show that  $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$  are irreducible elements in  $\mathbb{Z}[\sqrt{-5}]$ .

**Strategy:** For (a), verify ring axioms directly. For (b), show that complex conjugation preserves the structure of  $R$ . For (c), use the norm function to show that units must have norm 1. For (d), use the norm to show that these elements cannot be factored into non-units.

**Solution:**

- We need to show that  $R$  is closed under addition and multiplication. Let  $\alpha = a + b\sqrt{-D}$  and  $\beta = c + d\sqrt{-D}$  be elements of  $R$ .

Then  $\alpha + \beta = (a + c) + (b + d)\sqrt{-D} \in R$  and  $\alpha\beta = (ac - bdD) + (ad + bc)\sqrt{-D} \in R$ .

Also,  $0 = 0 + 0\sqrt{-D} \in R$  and  $1 = 1 + 0\sqrt{-D} \in R$ . Therefore,  $R$  is a ring.

- Complex conjugation is the map  $\sigma : \mathbb{C} \rightarrow \mathbb{C}$  defined by  $\sigma(a + bi) = a - bi$ . This is an automorphism of  $\mathbb{C}$ .

For  $\alpha = a + b\sqrt{-D} \in R$ , we have  $\sigma(\alpha) = a - b\sqrt{-D} \in R$ . Since  $\sigma$  preserves addition and multiplication, it induces an automorphism of  $R$ .

- Let  $\alpha = a + b\sqrt{-D}$  be a unit in  $R$ . Then there exists  $\beta = c + d\sqrt{-D} \in R$  such that  $\alpha\beta = 1$ .

Taking norms:  $N(\alpha)N(\beta) = N(1) = 1$ . Since  $N(\alpha) = a^2 + Db^2 \geq 0$  and  $N(\beta) = c^2 + Dd^2 \geq 0$ , we must have  $N(\alpha) = N(\beta) = 1$ .

If  $D \geq 2$ , then  $N(\alpha) = a^2 + Db^2 = 1$  implies  $b = 0$  and  $a^2 = 1$ . Therefore,  $\alpha = \pm 1$ .



(d) We show that these elements are irreducible in  $\mathbb{Z}[\sqrt{-5}]$ .

For 3: If  $3 = \alpha\beta$  where  $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$  are non-units, then  $N(3) = 9 = N(\alpha)N(\beta)$ . Since  $\alpha, \beta$  are non-units,  $N(\alpha), N(\beta) > 1$ . The only possibility is  $N(\alpha) = N(\beta) = 3$ . But there are no elements in  $\mathbb{Z}[\sqrt{-5}]$  with norm 3 (since  $a^2 + 5b^2 = 3$  has no integer solutions). Therefore, 3 is irreducible.

For  $2 + \sqrt{-5}$ :  $N(2 + \sqrt{-5}) = 4 + 5 = 9$ . If  $2 + \sqrt{-5} = \alpha\beta$  where  $\alpha, \beta$  are non-units, then  $N(\alpha) = N(\beta) = 3$ , which is impossible as above. Therefore,  $2 + \sqrt{-5}$  is irreducible.

Similarly,  $2 - \sqrt{-5}$  is irreducible.

■

## 2.5 Trigonometric Polynomials

### Definitions and Theorems:

- A **trigonometric polynomial** is a finite linear combination of functions  $\cos(nx)$  and  $\sin(nx)$  for non-negative integers  $n$ .
- The **trigonometric degree** of a trigonometric polynomial is the maximum frequency appearing in its expression.
- A **zero divisor** in a ring is a non-zero element  $a$  such that there exists a non-zero element  $b$  with  $ab = 0$ .
- An **irreducible element** in a ring is a non-zero non-unit that cannot be written as a product of two non-units.

### 2.11: Trigonometric Polynomial Ring

Let  $R$  be the ring of trigonometric polynomials as defined in the text. Show that  $R$  consists of all functions  $f$  on  $\mathbb{R}$  which have an expression of the form

$$f(x) = a_0 + \sum_{m=1}^n (a_m \cos mx + b_m \sin mx),$$

where  $a_0, a_m, b_m$  are real numbers. Define the trigonometric degree  $\deg_{tr}(f)$  to be the maximum of the integers  $r, s$  such that  $a_r, b_s \neq 0$ . Prove that

$$\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g).$$

Deduce from this that  $R$  has no divisors of 0, and also deduce that the functions  $\sin x$  and  $1 - \cos x$  are irreducible elements in that ring.

**Strategy:** Use trigonometric identities to show that multiplication of trigonometric polynomials adds their degrees. Use this degree property to show that the product of non-zero elements is non-zero (no zero divisors), and that elements of degree 1 cannot be factored into non-constant elements.

**Solution:** First, we show that  $R$  consists of all functions of the given form. This follows from the fact that any trigonometric polynomial can be written as a finite linear combination of  $\cos(nx)$  and  $\sin(nx)$  terms.

Now we prove that  $\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$ .

Let  $f(x) = a_0 + \sum_{m=1}^n (a_m \cos mx + b_m \sin mx)$  and  $g(x) = c_0 + \sum_{k=1}^p (c_k \cos kx + d_k \sin kx)$ .

When we multiply  $f$  and  $g$ , we get terms of the form:

$$\cos(mx) \cos(kx) = \frac{1}{2}(\cos((m+k)x) + \cos((m-k)x))$$

$$\cos(mx) \sin(kx) = \frac{1}{2}(\sin((m+k)x) + \sin((m-k)x))$$

$$\sin(mx) \cos(kx) = \frac{1}{2}(\sin((m+k)x) - \sin((m-k)x))$$

$$\sin(mx) \sin(kx) = \frac{1}{2}(-\cos((m+k)x) + \cos((m-k)x))$$

The highest frequency that can appear is  $m+k$  where  $m$  is the highest frequency in  $f$  and  $k$  is the highest frequency in  $g$ . Therefore,  $\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$ .

Since  $\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g)$ , if  $f$  and  $g$  are non-zero, then  $\deg_{tr}(fg) > 0$ , so  $fg \neq 0$ . This shows that  $R$  has no zero divisors.

For irreducibility, suppose  $\sin x = fg$  where  $f, g \in R$  are non-units. Then  $\deg_{tr}(f) + \deg_{tr}(g) = \deg_{tr}(\sin x) = 1$ . Since  $\deg_{tr}(f), \deg_{tr}(g) \geq 0$ , one of them must be 0 and the other must be 1. But if  $\deg_{tr}(f) = 0$ , then  $f$  is a constant, and if  $\deg_{tr}(g) = 0$ , then  $g$  is a constant. Since  $\sin x$  is not a constant multiple of any other trigonometric polynomial, this is impossible. Therefore,  $\sin x$  is irreducible.

Similarly,  $\deg_{tr}(1 - \cos x) = 1$ , so if  $1 - \cos x = fg$ , then one of  $f$  or  $g$  must be a constant. But  $1 - \cos x$  is not a constant multiple of any other trigonometric polynomial, so it is irreducible. ■

## 2.6 Dedekind Rings

### Definitions and Theorems:

- A **Dedekind ring** is a Noetherian integral domain that is integrally closed and has Krull dimension 1.
- A **multiplicative function**  $f$  satisfies  $f(mn) = f(m)f(n)$  whenever  $\gcd(m, n) = 1$ .
- The **Möbius function**  $\mu(n)$  is defined as  $\mu(1) = 1$ ,  $\mu(p_1 \cdots p_r) = (-1)^r$  for distinct primes  $p_i$ , and  $\mu(n) = 0$  if  $n$  is divisible by a square.
- The **convolution** of two arithmetic functions  $f$  and  $g$  is  $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$ .

Prove the following statements about a Dedekind ring  $o$ . To simplify terminology, by an ideal we shall mean non-zero ideal unless otherwise specified. We let  $K$  denote the quotient field of  $o$ ,

### 2.12: Ring of Arithmetic Functions

Let  $P$  be the set of positive integers and  $R$  the set of functions defined on  $P$  with values in a commutative ring  $K$ . Define the sum in  $R$  to be the ordinary addition of functions, and define the convolution product by the formula

$$(f * g)(m) = \sum_{xy=m} f(x)g(y),$$

where the sum is taken over all pairs  $(x, y)$  of positive integers such that  $xy = m$ .

- (a) Show that  $R$  is a commutative ring, whose unit element is the function  $\delta$  such that  $\delta(1) = 1$  and  $\delta(x) = 0$  if  $x \neq 1$ .

- (b) A function  $f$  is said to be multiplicative if  $f(mn) = f(m)f(n)$  whenever  $m, n$  are relatively prime. If  $f, g$  are multiplicative, show that  $f * g$  is multiplicative.
- (c) Let  $\mu$  be the Möbius function such that  $\mu(1) = 1$ ,  $\mu(p_1 \cdots p_r) = (-1)^r$  if  $p_1, \dots, p_r$  are distinct primes, and  $\mu(m) = 0$  if  $m$  is divisible by  $p^2$  for some prime  $p$ . Show that  $\mu * \varphi_1 = \delta$ , where  $\varphi_1$  denotes the constant function having value 1. [Hint: Show first that  $\mu$  is multiplicative, and then prove the assertion for prime powers.] The Möbius inversion formula of elementary number theory is then nothing else but the relation  $\mu * \varphi_1 * f = f$ .

**Strategy:** For (a), verify ring axioms directly using the convolution definition. For (b), use the fact that if  $m, n$  are coprime, then any divisor of  $mn$  can be written uniquely as a product of a divisor of  $m$  and a divisor of  $n$ . For (c), first show  $\mu$  is multiplicative, then use multiplicativity to reduce to checking the identity on prime powers.

**Solution:**

- (a) We need to verify the ring axioms. Addition is clearly commutative and associative since it's pointwise addition.

For multiplication, we check associativity:

$$\begin{aligned} ((f * g) * h)(m) &= \sum_{xy=m} (f * g)(x)h(y) = \sum_{xy=m} \sum_{ab=x} f(a)g(b)h(y) \\ &= \sum_{aby=m} f(a)g(b)h(y) = \sum_{abc=m} f(a)g(b)h(c) \end{aligned}$$

Similarly,  $(f * (g * h))(m) = \sum_{abc=m} f(a)g(b)h(c)$ , so convolution is associative.

The distributive law follows from:

$$\begin{aligned} (f * (g + h))(m) &= \sum_{xy=m} f(x)(g + h)(y) = \sum_{xy=m} f(x)(g(y) + h(y)) \\ &= \sum_{xy=m} f(x)g(y) + \sum_{xy=m} f(x)h(y) = (f * g)(m) + (f * h)(m) \end{aligned}$$

The function  $\delta$  is the unit since  $(\delta * f)(m) = \sum_{xy=m} \delta(x)f(y) = f(m)$ .

(b) Let  $m, n$  be relatively prime positive integers. Then:

$$\begin{aligned}
 (f * g)(mn) &= \sum_{xy=mn} f(x)g(y) = \sum_{a_1 a_2 = m, b_1 b_2 = n} f(a_1 b_1)g(a_2 b_2) \\
 &= \sum_{a_1 a_2 = m, b_1 b_2 = n} f(a_1)f(b_1)g(a_2)g(b_2) \\
 &= \left( \sum_{a_1 a_2 = m} f(a_1)g(a_2) \right) \left( \sum_{b_1 b_2 = n} f(b_1)g(b_2) \right) \\
 &= (f * g)(m)(f * g)(n)
 \end{aligned}$$

(c) First, we show that  $\mu$  is multiplicative. Let  $m, n$  be relatively prime. If either  $m$  or  $n$  is divisible by a square, then  $\mu(mn) = 0 = \mu(m)\mu(n)$ . Otherwise, if  $m = p_1 \cdots p_r$  and  $n = q_1 \cdots q_s$  are products of distinct primes, then  $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$ .

Now we show that  $\mu * \varphi_1 = \delta$ . Since both  $\mu$  and  $\varphi_1$  are multiplicative, so is  $\mu * \varphi_1$ . Therefore, it suffices to check the equality for prime powers.

For  $p^k$  where  $k \geq 1$ :

$$\begin{aligned}
 (\mu * \varphi_1)(p^k) &= \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\
 &= 1 + (-1) + 0 + \cdots + 0 = 0
 \end{aligned}$$

For  $m = 1$ :  $(\mu * \varphi_1)(1) = \mu(1) = 1$ .

Therefore,  $\mu * \varphi_1 = \delta$ . ■

### 2.13: Finitely Generated Ideals

Every ideal is finitely generated. [Hint: Given an ideal  $\mathfrak{a}$ , let  $\mathfrak{b}$  be the fractional ideal such that  $\mathfrak{a}\mathfrak{b} = \mathfrak{o}$ . Write  $1 = \sum a_i b_i$  with  $a_i \in \mathfrak{a}$  and  $b_i \in \mathfrak{b}$ . Show that  $\mathfrak{a} = (a_1, \dots, a_n)$ .]

**Strategy:** Use the fact that in a Dedekind ring, every ideal has an inverse fractional ideal. Write 1 as a finite sum using elements from  $\mathfrak{a}$

and its inverse, then show that any element of  $\mathfrak{a}$  can be written as a linear combination of the  $a_i$ .

**Solution:** Let  $\mathfrak{a}$  be an ideal of  $o$ . Since  $o$  is a Dedekind ring, there exists a fractional ideal  $\mathfrak{b}$  such that  $\mathfrak{a}\mathfrak{b} = o$ .

Since  $1 \in o = \mathfrak{a}\mathfrak{b}$ , we can write  $1 = \sum_{i=1}^n a_i b_i$  where  $a_i \in \mathfrak{a}$  and  $b_i \in \mathfrak{b}$ .

We claim that  $\mathfrak{a} = (a_1, \dots, a_n)$ .

Let  $a \in \mathfrak{a}$ . Then  $a = a \cdot 1 = a \sum_{i=1}^n a_i b_i = \sum_{i=1}^n (a b_i) a_i$ .

Since  $a \in \mathfrak{a}$  and  $b_i \in \mathfrak{b}$ , we have  $a b_i \in \mathfrak{a}\mathfrak{b} = o$ . Therefore,  $a b_i \in o$  for each  $i$ .

This shows that  $a = \sum_{i=1}^n (a b_i) a_i \in (a_1, \dots, a_n)$ .

Therefore,  $\mathfrak{a} = (a_1, \dots, a_n)$  is finitely generated. ■

### 2.14: Unique Factorization of Ideals

Every ideal has a factorization as a product of prime ideals, uniquely determined up to permutation.

**Strategy:** This is a fundamental property of Dedekind rings. For existence, use the fact that every ideal is contained in a maximal ideal and the Noetherian property. For uniqueness, use the fact that prime ideals are maximal and the prime ideal property.

**Solution:** This is a fundamental property of Dedekind rings. We prove existence and uniqueness.

For existence: Let  $\mathfrak{a}$  be an ideal. If  $\mathfrak{a} = o$ , then it's the empty product. Otherwise, let  $\mathfrak{p}_1$  be a minimal prime ideal containing  $\mathfrak{a}$ . Then  $\mathfrak{a} \subseteq \mathfrak{p}_1$ , so there exists an ideal  $\mathfrak{a}_1$  such that  $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1$ . Since  $\mathfrak{p}_1$  is maximal (in Dedekind rings, non-zero prime ideals are maximal),  $\mathfrak{a}_1$  properly contains  $\mathfrak{a}$ . Continue this process, which must terminate since  $o$  is Noetherian.

For uniqueness: Suppose  $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$  where the  $\mathfrak{p}_i$  and  $\mathfrak{q}_j$  are prime ideals. Since  $\mathfrak{p}_1$  contains the product  $\mathfrak{q}_1 \cdots \mathfrak{q}_s$ , it must contain one of the  $\mathfrak{q}_j$  (by the prime ideal property). Since both are maximal,  $\mathfrak{p}_1 = \mathfrak{q}_j$ . Cancel and continue by induction. ■

**2.15: Principal Prime Ideal**

Suppose  $\mathfrak{o}$  has only one prime ideal  $\mathfrak{p}$ . Let  $t \in \mathfrak{p}$  and  $t \notin \mathfrak{p}^2$ . Then  $\mathfrak{p} = (t)$  is principal.

**Strategy:** Use the unique factorization property of ideals in a Dedekind ring. Since there's only one prime ideal, every non-zero element has a unique factorization as a power of  $\mathfrak{p}$ . The condition  $t \in \mathfrak{p}$  but  $t \notin \mathfrak{p}^2$  forces  $(t) = \mathfrak{p}$ .

**Solution:** Since  $\mathfrak{o}$  has only one prime ideal  $\mathfrak{p}$ , every non-zero element of  $\mathfrak{o}$  has a unique factorization as a power of  $\mathfrak{p}$ .

Since  $t \in \mathfrak{p}$  and  $t \notin \mathfrak{p}^2$ , the ideal  $(t)$  must be exactly  $\mathfrak{p}$ .

To see this, suppose  $(t) = \mathfrak{p}^n$  for some  $n \geq 1$ . Since  $t \notin \mathfrak{p}^2$ , we must have  $n = 1$ . Therefore,  $(t) = \mathfrak{p}$ . ■

**2.16: Localization of Dedekind Ring**

Let  $\mathfrak{o}$  be any Dedekind ring. Let  $\mathfrak{p}$  be a prime ideal. Let  $\mathfrak{o}_{\mathfrak{p}}$  be the local ring at  $\mathfrak{p}$ . Then  $\mathfrak{o}_{\mathfrak{p}}$  is Dedekind and has only one prime ideal.

**Strategy:** Show that localization preserves the three defining properties of a Dedekind ring: Noetherian, integrally closed, and Krull dimension 1. Then use the fact that localization at a prime ideal creates a local ring with unique maximal ideal.

**Solution:** Let  $S = \mathfrak{o} \setminus \mathfrak{p}$ . Then  $\mathfrak{o}_{\mathfrak{p}} = S^{-1}\mathfrak{o}$ .

Since  $\mathfrak{o}$  is Noetherian,  $\mathfrak{o}_{\mathfrak{p}}$  is Noetherian. Since  $\mathfrak{o}$  is integrally closed,  $\mathfrak{o}_{\mathfrak{p}}$  is integrally closed. Since  $\mathfrak{o}$  has Krull dimension 1,  $\mathfrak{o}_{\mathfrak{p}}$  has Krull dimension 1.

Therefore,  $\mathfrak{o}_{\mathfrak{p}}$  is a Dedekind ring.

The unique prime ideal of  $\mathfrak{o}_{\mathfrak{p}}$  is  $\mathfrak{p}\mathfrak{o}_{\mathfrak{p}} = \{a/s : a \in \mathfrak{p}, s \notin \mathfrak{p}\}$ . This follows from the fact that localization preserves the prime ideal structure, and in a local ring, the unique maximal ideal is the only prime ideal. ■

### 2.17: Divisibility in Dedekind Rings

As for the integers, we say that  $\mathfrak{a}|\mathfrak{b}$  ( $\mathfrak{a}$  divides  $\mathfrak{b}$ ) if there exists an ideal  $\mathfrak{c}$  such that  $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ . Prove:

- (a)  $\mathfrak{a}|\mathfrak{b}$  if and only if  $\mathfrak{b} \subseteq \mathfrak{a}$ .
- (b) Let  $\mathfrak{a}, \mathfrak{b}$  be ideals. Then  $\mathfrak{a} + \mathfrak{b}$  is their greatest common divisor. In particular,  $\mathfrak{a}, \mathfrak{b}$  are relatively prime if and only if  $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ .

**Strategy:** For (a), use the fact that every ideal has an inverse fractional ideal in a Dedekind ring. For (b), show that  $\mathfrak{a} + \mathfrak{b}$  is the smallest ideal containing both  $\mathfrak{a}$  and  $\mathfrak{b}$ , which makes it the greatest common divisor.

**Solution:**

- (a) If  $\mathfrak{a}|\mathfrak{b}$ , then  $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$  for some ideal  $\mathfrak{c}$ . Since  $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$ , we have  $\mathfrak{b} \subseteq \mathfrak{a}$ .

Conversely, if  $\mathfrak{b} \subseteq \mathfrak{a}$ , then there exists a fractional ideal  $\mathfrak{c}$  such that  $\mathfrak{a}\mathfrak{c} = \mathfrak{o}$ . Then  $\mathfrak{b} = \mathfrak{b}\mathfrak{o} = \mathfrak{b}(\mathfrak{a}\mathfrak{c}) = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$ . Since  $\mathfrak{b}\mathfrak{c}$  is an ideal, we have  $\mathfrak{a}|\mathfrak{b}$ .

- (b) We need to show that  $\mathfrak{a} + \mathfrak{b}$  is the smallest ideal containing both  $\mathfrak{a}$  and  $\mathfrak{b}$ .

Clearly,  $\mathfrak{a} + \mathfrak{b}$  contains both  $\mathfrak{a}$  and  $\mathfrak{b}$ . If  $\mathfrak{c}$  is any ideal containing both  $\mathfrak{a}$  and  $\mathfrak{b}$ , then  $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$ .

Therefore,  $\mathfrak{a} + \mathfrak{b}$  is the greatest common divisor of  $\mathfrak{a}$  and  $\mathfrak{b}$ .

Two ideals are relatively prime if their greatest common divisor is  $\mathfrak{o}$ . By the above, this means  $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ .

■

### 2.18: Prime Ideals are Maximal

Every prime ideal  $\mathfrak{p}$  is maximal. (Remember,  $\mathfrak{p} \neq 0$  by convention.) In particular, if  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  are distinct primes, then the Chinese remainder theorem applies to their powers  $\mathfrak{p}_1^{r_1}, \dots, \mathfrak{p}_n^{r_n}$ . Use this to prove:

**Strategy:** Use the definition of Krull dimension 1, which means that every non-zero prime ideal is maximal. If there were a chain of prime ideals  $(0) \subset \mathfrak{p} \subset \mathfrak{m}$ , it would contradict the Krull dimension being 1.



**Solution:** Since  $\mathfrak{o}$  is a Dedekind ring, it has Krull dimension 1. This means that every non-zero prime ideal is maximal.

To see this, let  $\mathfrak{p}$  be a non-zero prime ideal. If  $\mathfrak{p}$  is not maximal, then there exists a maximal ideal  $\mathfrak{m}$  such that  $\mathfrak{p} \subset \mathfrak{m}$ . But this would create a chain of prime ideals  $(0) \subset \mathfrak{p} \subset \mathfrak{m}$ , contradicting the fact that the Krull dimension is 1.

Since prime ideals are maximal, distinct prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  are pairwise coprime. Therefore, the Chinese remainder theorem applies to their powers  $\mathfrak{p}_1^{r_1}, \dots, \mathfrak{p}_n^{r_n}$ .

This means that the natural map  $\mathfrak{o} \rightarrow \mathfrak{o}/\mathfrak{p}_1^{r_1} \times \dots \times \mathfrak{o}/\mathfrak{p}_n^{r_n}$  is surjective. ■

### 2.19: Ideal Class Representatives

Let  $\mathfrak{a}, \mathfrak{b}$  be ideals. Show that there exists an element  $c \in K$  (the quotient field of  $\mathfrak{o}$ ) such that  $c\mathfrak{a}$  is an ideal relatively prime to  $\mathfrak{b}$ . In particular, every ideal class in  $\text{Pic}(\mathfrak{o})$  contains representative ideals prime to a given ideal. For a continuation, see Exercise 7 of Chapter VII; Chapter III, Exercise 11-13.

**Strategy:** Use the unique factorization of ideals to write  $\mathfrak{a}$  and  $\mathfrak{b}$  as products of prime ideals. Choose  $c$  to be a product of elements from prime ideals that appear in  $\mathfrak{a}$  but not in  $\mathfrak{b}$ , so that  $c\mathfrak{a}$  has no prime factors in common with  $\mathfrak{b}$ .

**Solution:** Let  $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$  and  $\mathfrak{b} = \mathfrak{q}_1^{f_1} \dots \mathfrak{q}_s^{f_s}$  be the prime factorizations of  $\mathfrak{a}$  and  $\mathfrak{b}$ .

We need to find  $c \in K$  such that  $c\mathfrak{a}$  is relatively prime to  $\mathfrak{b}$ . This means that  $c\mathfrak{a}$  should not share any prime factors with  $\mathfrak{b}$ .

Let  $c = \prod_{i=1}^r \mathfrak{p}_i^{-e_i}$ . Then  $c\mathfrak{a} = \mathfrak{o}$ , which is relatively prime to any ideal.

However, this  $c$  might not be in  $K$  in the sense that  $c\mathfrak{a}$  might not be an ideal. Instead, we can choose  $c$  to be a product of elements from the prime ideals that appear in  $\mathfrak{a}$  but not in  $\mathfrak{b}$ .

More precisely, let  $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \setminus \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\}$  be the set of prime ideals that appear in  $\mathfrak{a}$  but not in  $\mathfrak{b}$ .

For each  $\mathfrak{p} \in S$ , choose an element  $t_{\mathfrak{p}} \in \mathfrak{p} \setminus \mathfrak{p}^2$ . Let  $c = \prod_{\mathfrak{p} \in S} t_{\mathfrak{p}}^{e_{\mathfrak{p}}}$  where  $e_{\mathfrak{p}}$  is the exponent of  $\mathfrak{p}$  in the factorization of  $\mathfrak{a}$ .

Then  $c\mathfrak{a}$  will have the same prime factors as  $\mathfrak{a}$  except for those in  $S$ , which means it will be relatively prime to  $\mathfrak{b}$ .

This shows that every ideal class in  $\text{Pic}(o)$  contains representative ideals prime to a given ideal.

## 2.7 Problem-Solving Techniques

### Proving Prime Ideals

- Use proof by contradiction: assume the ideal is not prime and find elements  $a, b$  with  $ab$  in the ideal but  $a, b$  not in it
- Use maximality properties: if an ideal is maximal with respect to certain conditions, it's often prime
- Use localization: localizing at a prime ideal creates a local ring with unique maximal ideal

### Proving Local Rings

- Show there is exactly one maximal ideal
- Use surjective homomorphisms: if  $f : A \rightarrow A'$  is surjective and  $A$  is local, then  $A'$  is local
- Use localization:  $A_{\mathfrak{p}}$  is always a local ring

### Proving Principal Rings

- Use Euclidean algorithm with a norm function (e.g., for  $\mathbb{Z}[i]$ )
- Show that every ideal is generated by a single element
- Use localization: if  $A$  is principal, then  $S^{-1}A$  is principal

### Proving Factorial Rings

- Show unique factorization of elements into irreducibles
- Use the fact that principal rings are factorial
- Use localization: if  $A$  is factorial, then  $S^{-1}A$  is factorial

### Proving Irreducibility

- Use norm functions in quadratic rings to show elements cannot be factored
- Use degree functions (e.g., trigonometric degree) to show elements cannot be factored
- Show that any factorization would require one factor to be a unit

### Working with Dedekind Rings

1. Use unique factorization of ideals into prime ideals
2. Use the fact that every ideal has an inverse fractional ideal
3. Use the fact that prime ideals are maximal (Krull dimension 1)
4. Use localization to reduce to local rings with single prime ideal

### Proving Divisibility

- In Dedekind rings:  $\mathfrak{a}|\mathfrak{b}$  if and only if  $\mathfrak{b} \subseteq \mathfrak{a}$
- Use greatest common divisors:  $\mathfrak{a} + \mathfrak{b}$  is the GCD of ideals  $\mathfrak{a}$  and  $\mathfrak{b}$
- Use the fact that ideals are relatively prime if and only if their sum is the whole ring

### Working with Units

- Use norm functions to find units in quadratic rings
- Use the structure of multiplicative groups modulo prime powers
- For  $\mathbb{Z}/p^r\mathbb{Z}$ , use induction and exact sequences

### Proving Ring Properties

- Verify ring axioms directly (closure, associativity, distributivity)
- Use homomorphisms to transfer properties between rings
- Use localization to transfer properties from a ring to its localizations

# Chapter 3

## Modules

### 3.1 Discrete Distributions

#### 3.1: Discrete Uniform Distribution

Let  $X$  be a random variable with the general discrete uniform( $N_0, N_1$ ) distribution that puts equal probability on each of the values  $N_0, N_0 + 1, \dots, N_1$ . Here  $N_0 \leq N_1$  and both are integers. Find expressions for  $EX$  and  $\text{Var}X$ .

#### 3.2: Acceptance Sampling

A manufacturer receives a lot of 100 parts from a vendor. The lot will be unacceptable if more than five of the parts are defective. The manufacturer is going to select randomly  $K$  parts from the lot for inspection and the lot will be accepted if no defective parts are found in the sample.

- (a) How large does  $K$  have to be to ensure that the probability that the manufacturer accepts an unacceptable lot is less than .10?
- (b) Suppose the manufacturer decides to accept the lot if there is at most one defective in the sample. How large does  $K$  have to be to ensure that the probability that the manufacturer accepts an unacceptable lot is less than .10?

**3.3: Bernoulli Trials in Traffic**

The flow of traffic at certain street corners can sometimes be modeled as a sequence of Bernoulli trials by assuming that the probability of a car passing during any given second is a constant  $p$  and that there is no interaction between the passing of cars at different seconds. Treating seconds as indivisible time units (trials), the Bernoulli model applies. Suppose a pedestrian can cross the street only if no car is to pass during the next three seconds. Find the probability that the pedestrian has to wait for exactly four seconds before starting to cross.

**3.4: Key Trials**

A man with  $n$  keys wants to open his door and tries the keys at random. Exactly one key will open the door. Find the mean number of trials if

- (a) unsuccessful keys are not eliminated from further selections.
- (b) unsuccessful keys are eliminated.

## 3.2 Binomial and Poisson Distributions

**3.5: Drug Effectiveness**

A standard drug is known to be effective in 80% of the cases in which it is used. A new drug is tested on 100 patients and found to be effective in 85 cases. Is the new drug superior? (Hint: Evaluate the probability of observing 85 or more successes assuming that the new and old drugs are equally effective.)

**3.6: Insect Survival**

A large number of insects are expected to be attracted to a certain variety of rose plant. A commercial insecticide is advertised as being 99% effective. Suppose 2,000 insects infest a rose garden where the insecticide has been applied, and let  $X = \#$  of surviving insects.

- (a) What probability distribution might provide a reasonable model for this experiment?
- (b) Write down, but do not evaluate, an expression for the probability that fewer than 100 insects survive, using the model in part (a).
- (c) Evaluate an approximation to the probability in part (b).

**3.7: Poisson Chocolate Chips**

Let the number of chocolate chips in a certain type of cookie have a Poisson distribution. We want the probability that a randomly chosen cookie has at least two chocolate chips to be greater than .99. Find the smallest value of the mean of the distribution that ensures this probability.

### 3.3 Normal Approximations

**3.8: Theater Competition**

Two movie theaters compete for the business of 1,000 customers. Assume that each customer chooses between the movie theaters independently and with “indifference.” Let  $N$  denote the number of seats in each theater.

- (a) Using a binomial model, find an expression for  $N$  that will guarantee that the probability of turning away a customer (because of a full house) is less than 1%.
- (b) Use the normal approximation to get a numerical value for  $N$ .

## 3.4 Exponential Families

**3.28: Exponential Family Verification**

Show that each of the following families is an exponential family.

- (a) normal family with either parameter  $\mu$  or  $\sigma$  known
- (b) gamma family with either parameter  $\alpha$  or  $\beta$  known or both unknown
- (c) beta family with either parameter  $\alpha$  or  $\beta$  known or both unknown
- (d) Poisson family
- (e) negative binomial family with  $r$  known,  $0 < p < 1$

## 3.5 Inequalities

**3.44: Markov and Chebychev Bounds**

For any random variable  $X$  for which  $EX^2$  and  $E|X|$  exist, show that  $P(|X| \geq b)$  does not exceed either  $EX^2/b^2$  or  $E|X|/b$ , where  $b$  is a positive constant. If  $f(x) = e^{-x}$  for  $x > 0$ , show that one bound is

better when  $b = 3$  and the other when  $b = \sqrt{2}$ . (Notice Markov's Inequality Miscellanea 3.8.2.)

### 3.46: Chebychev Applications

Calculate  $P(|X - \mu_X| \geq k\sigma_X)$  for  $X \sim \text{uniform}(0, 1)$  and  $X \sim \text{exponential}(\lambda)$ , and compare your answers to the bound from Chebychev's Inequality.

## 3.6 Miscellaneous

### 3.25: Hazard Function

Suppose the random variable  $T$  is the length of life of an object (possibly the lifetime of an electrical component or of a subject given a particular treatment). The hazard function  $h_T(t)$ , associated with the random variable  $T$ , is defined by

$$h_T(t) = \lim_{\delta \rightarrow 0} \frac{P(t \leq T < t + \delta | T \geq t)}{\delta}.$$

Thus, we can interpret  $h_T(t)$  as the rate of change of the probability that the object survives a little past time  $t$ , given that the object survives to time  $t$ . Show that if  $T$  is a continuous random variable, then

$$h_T(t) = \frac{f_T(t)}{1 - F_T(t)} = -\frac{d}{dt} \log(1 - F_T(t)).$$

### 3.26: Hazard Function Verification

Verify that the following pdfs have the indicated hazard functions (see Exercise 3.25).



- (a) If  $T \sim \text{exponential}(\beta)$ , then  $h_T(t) = 1/\beta$ .
- (b) If  $T \sim \text{Weibull}(\gamma, \beta)$ , then  $h_T(t) = (\gamma/\beta)t^{\gamma-1}$ .
- (c) If  $T \sim \text{logistic}(\mu, \beta)$ , that is,

$$F_T(t) = \frac{1}{1 + e^{-(t-\mu)/\beta}},$$

then  $h_T(t) = (1/\beta)F_T(t)$ .