Group Theory

Problems and Solutions in Group Theory

Konstantinos Bizanos

May 31, 2026

Athens, Greece

Preface

This file is a collection of exercises in Group Theory. The range of the exercises covers the material of the undergraduate course Group Theory as well as of the graduate course Algebra I. The majority of the exercises are from the corresponding exercise sheets of the instructor M. Sykiotis from the academic years Winter semester 2020–21 (undergraduate group theory) and Winter semester 2022–23 (graduate Algebra I). This file is far from being well written, but as a small excuse for possible mistakes, let us note that the file is not intended to replace individual study and effort, but to support it. So let us call possible mistakes "food for thought".

Nevertheless, if you notice any typographical mistake, or any other kind of mistake, I would be happy for you to point it out to me by email at kostasbizanos@gmail.com or at kbfg6@missouri.edu

Contents

Chapter 1

The Concept of a Group

Problem 1.1. If H, K are subgroups of finite index of a group G with $K \leq H$, then

$$[G : K] = [G : H] \cdot [K : H].$$

We assume that $[G : K] < \infty$.

Solution. Let $T_1 = \{g_1, \ldots, g_n\}$ be a set of representatives of H in G, and let $T_2 = \{x_1, \ldots, x_m\}$ be a set of representatives of K in H. Then

$$T = \{g_i x_j \mid g_i \in T_1, x_j \in T_2\}$$

is a set of representatives of K in G. ■

Problem 1.2. Prove that if $H, K \leq G$ with $[G : H] = m$ and $[G : K] = n$, then $[G : H \cap K] \geq$ l.c.m.(m, n). Moreover, we have equality if $(m, n) = 1$. Moreover, assume that $(m, n) = 1$, hence we have that $mn|[G : H \cap K]$.

Solution. We have that

$$[G : H \cap K] = [G : K] \cdot [K : H \cap K] \Rightarrow n|[G : H \cap K].$$

Similarly, it holds that $n|[G : H \cap K]$, therefore we have that l.c.m.$(m, n)|[G : H \cap K]$. It remains to show that $[K : H \cap K] \leq m$, and from the initial relation we will have the desired result. Consider the map

$$\varphi\colon K/H \cap K \to G/H, \quad kH \cap K \mapsto kH.$$

which is one-to-one. Hence, we have that $[K : H \cap K] \leq m$, hence from the initial relation $[G : H \cap K] \leq mn$. ■

Problem 1.3. Prove that if $H_1, \dots, H_n$ are subgroups of G of finite index, then their intersection is also of finite index in G, and

$$\left[G : \bigcap_{i=1}^{n} H_i\right] \leq \prod_{i=1}^{n} [G : H_i].$$

Solution. Consider the map

$$\varphi\colon G/\bigcap_{i=1}^{n} H_i \to \prod_{i=1}^{n} G/H_i, \quad g\bigcap_{i} H_i \mapsto (gH_1, \dots, gH_n)$$

and show that it is one-to-one. ■

Problem 1.4. Let H, K be a pair of subgroups of a group G. The product $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G if and only if $HK = KH$.

Solution. Suppose that $HK \leq G$. Then we have that $KH \leq G$ (why?). Let $hk \in HK$. Since $(hk)^{-1} = k^{-1}h^{-1} \in KH$ and $KH \leq G$, then we have that $hk \in KH$. Similarly, show that $KH \subseteq HK$.

Conversely, suppose that $HK = KH$. We will show that $HK \leq G$. Let $h_1k_1, h_2k_2 \in HK$. Then

$$(h_2k_2)^{-1}(h_1k_1) = k_2^{-1}h_2^{-1}h_1k_1.$$

Since $k_2^{-1}h_2^{-1}h_1 \in KH$, then there exist $\tilde{k} \in K, \tilde{h} \in H$ such that

$$k_2^{-1}h_2^{-1}h_1 = \tilde{h}\tilde{k}.$$

Thus we have that

$$(h_2k_2)^{-1}(h_1k_1) = \tilde{h}\tilde{k}k_2 \in HK$$

and we have the desired result. ■

Problem 1.5. Let K be a finite cyclic subgroup of G and $K \lhd G$. Show that every subgroup of K is normal in G.

Solution. Let $K = \langle x \rangle$. Let $H \leq K$, that is, $H = \langle x^k \rangle$, and let $g \in G$. Then we have that

$$g^{-1}x^kg = \left(g^{-1}xg\right)^k \in H$$

and so we have the desired result. ■

Problem 1.6. Let $N \lhd G,\ g \in G$ and $|G/N| = n < \infty$. Assume that $(m,n) = 1$ and $g^m \in N$. Show that $g \in N$.

Solution. Since $(m,n) = 1$, there exist $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Hence,

$$gN = (g^m)^x\, N \cdot (g^n)^y\, N = N.$$

■

Problem 1.7. Let G be a group and $\mathrm{C}(G) = \{x \in G \mid gx = xg, \text{ for every } g \in G\}$ be the center of G. Prove that

(a) $\mathrm{C}(G)$ is an abelian normal subgroup of G.

(b) Every subgroup of the center is normal in G.

(c) If G is not abelian, then $G/\,\mathrm{C}(G)$ is not cyclic.

(d) If $K \lhd G$ and $|K| = 2$, then $K \leq \mathrm{C}(G)$.

(e) If $\varphi\colon G \to G_1$ is an epimorphism and $H \leq \mathrm{C}(G)$, then $\varphi(H) \leq \mathrm{C}(G_1)$.

(f) If $K \lhd G$, then $\mathrm{C}(G)/\,\mathrm{C}(G) \cap K$ is isomorphic to the group $\mathrm{C}(G/K)$.

Solution. (a) Immediate.

(b) Immediate.

(c) Suppose that $G/\,\mathrm{C}(G) = \langle g\,\mathrm{C}(G)\rangle$. Let $g_1, g_2 \in G$. Then there exist $m, n \in \mathbb{N}$ and $z_1, z_2 \in \mathrm{C}(G)$ such that $g_1 = g^m z_1$ and $g_2 = g^n z_2$. Show that $g_1 g_2 = g_2 g_1$.

(d) Initially, $K = \{1, k\}$ with $k \neq 1$. Then, for every $g \in G$, from the normality of K we have that $g^{-1}kg = k$, and we have the desired result.

(e) Immediate.

(f) Immediate.

■

Problem 1.8. Let G be a group and $g, h \in G$. The commutator of g, h is the element $[g,h] = g^{-1}h^{-1}gh$. The **derived group** G' of G is defined as the subgroup of G generated by all commutators of elements of G. Prove that:

(a) $G' \lhd G$.

(b) If $H \leq G$ and $G' \subseteq H$, then $H \lhd G$.

(c) If $H \lhd G$, then G/H is abelian if and only if $G' \leq H$. In particular, $G' \leq H$.

Solution. (a) Let $x \in G$. It is enough to show that $x^{-1}[g,h]x \in G'$, for every $g, h \in G$. Indeed, if $g, h \in G$, then

$$x^{-1}[g,h]x = x^{-1}h^{-1}g^{-x}ghx = [g, hx] \in G'.$$

(b) Let $g \in G$ and $h \in H$. Then $[g,h] \in H$, hence $g^{-1}hg \in H$.

(c) G/H is abelian if and only if $[g,h] \in H$, for every $g, h \in G$, if and only if $G' \leq H$. ∎

Problem 1.9. (a) Let G be a group and $\varphi\colon G \to G$ be a map such that $\varphi(g) = g^{-1}$, for every $g \in G$. Prove that φ is a homomorphism if and only if G is abelian.

(b) Let G be a finite group and $\vartheta\colon G \to G$ be an automorphism such that $\vartheta^2(g) = g$, for every $g \in G$. Assume moreover that if $g \in G$ and $\vartheta(g) = g$, then $g = 1$. Prove that $\vartheta(g) = g^{-1}$, for every $g \in G$, and consequently G is abelian.

Solution. (a) Immediate.

(b) Since the map $g \mapsto g^{-1}\vartheta(g)$ is one-to-one and onto, we have that

$$G = \left\{g^{-1}\vartheta(g) \mid g \in G\right\}.$$

Let $g \in G$. Then there exists $a \in G$ such that $g = a^{-1}\vartheta(a)$. Thus

$$\vartheta(g) = \vartheta(a^{-1})a = g^{-1}.$$

∎

Problem 1.10. Suppose that G is a finite group with the property $(ab)^n = a^n b^n$, for every $a, b \in G$, where n is a fixed integer greater than 1. Let $G_n = \{a \in G \mid a^n = 1\}$ and $G^n = \{g^n \mid g \in G\}$. Prove that G_n and G^n are normal subgroups of G and that $|G^n| = [G : G_n]$.

Solution. G_n is a normal subgroup of G as the kernel of the homomorphism $g \mapsto g^n$. Now, since $x^{-1}g^n x = (x^{-1}gx)^n$, we have that G^n is a normal subgroup of G. From the above homomorphism we also have the desired relation. ∎

Problem 1.11. Let G be a finite group and let K be a normal subgroup of G with $(G, [G : K]) = 1$. Show that K is the unique subgroup of G of order $|K|$.

Solution. Let $H \leq G$ with $|H| = |K|$. Consider the canonical projection $\pi\colon G \to G/K$. Then it holds that $|\pi(H)| \,\Big|\, [G : K]$ and $|\pi(H)| \,\Big|\, |K|$. Hence, we have that $\pi(H) = \{1\}$, that is, $H \subseteq \ker \pi = K$, and since they have equal orders it follows that $H = K$. ■

Problem 1.12. Let G be an abelian group and let p be a prime such that $o(g) = p$, for every $g \in G$. We consider the field $F = \mathbb{Z}_p$ and define operations

$$\oplus\colon G \times G \to G, \quad *\colon F \times G \to G$$

as follows: $g_1 \oplus g_2 = g_1 \cdot g_2$ and $[n] \cdot g = g^n$, where by $[n] \in \mathbb{Z}_p$ we denote the congruence class of n.

(a) Show that G, with the above operations, becomes a vector space over F. In particular, if G is finite, then $|G| = p^m$, where $m = \dim_F G$.

(b) If G is finite, then $\operatorname{Aut}(G) \cong \mathrm{GL}_m(\mathbb{Z}_p)$.

Solution. (a) The first part is immediate. If G is finite, then it is a finite-dimensional vector space with $\dim_F G = m$. Hence, there exists a basis $\{g_1, \ldots, g_m\}$ of G, where for every $g \in G$ there exist unique $[n_1], \ldots, [n_m] \in \mathbb{Z}_p$ such that

$$g = [n_1] \cdot g_1 \oplus \cdots \oplus [n_m] \cdot g_m = g_1^{n_1} \cdots g_m^{n_m}.$$

Hence, it is clear that $|G| = p^m$.

(b) Let $\{g_1, \ldots, g_m\}$ be a basis of the F-vector space G with the operations as in (a). Then, from (a), we observe that $\{g_1, \ldots, g_m\}$ is a set of generators for the group G, hence every automorphism of it is completely determined by the images of the generators. Let $\varphi \in \operatorname{Aut}(G)$. For every $i = 1, \ldots, m$, there exist unique $a_{i1}, \ldots, a_{im}$ such that $\varphi(g_i) = g_1^{a_{i1}} \cdots g_m^{a_{im}}$. We define $\psi\colon \operatorname{Aut}(G) \to \mathrm{GL}_m(\mathbb{Z}_p)$ by

$$\psi(\varphi) = \begin{pmatrix} [a_{11}] & [a_{21}] & \cdots & [a_{m1}] \\ \vdots & \vdots & & \vdots \\ [a_{1m}] & [a_{2m}] & \cdots & [a_{mm}] \end{pmatrix}$$

The map ψ is well-defined, since every $\varepsilon \in \operatorname{Aut}(G)$ is also a linear isomorphism of G, hence it maps every basis to a basis. Hence, the columns of the above matrix are linearly independent, that is, the matrix is invertible. Now, it is immediate that ψ is a group isomorphism.

■

Problem 1.13. Let F be a field and let G be a finite group. Show that G is isomorphic to a subgroup of the general linear group $\mathrm{GL}_n(F)$, for some $n \leq |G|$.

Problem 1.14. Let G be a finitely generated group and let S be a finite set of generators of G. We define $\|\cdot\|_S\colon G \to [0,\infty)$ as follows: $\|1_G\|_S = 0$ and, for $1_G \neq g$,

$$\|g\|_S = \min\left\{n \in \mathbb{N} \mid g = s_{i_1}^{\varepsilon_1}\cdots s_{i_n}^{\varepsilon_n}, \text{ where } s_{i_j} \in S \cup S^{-1} \text{ and } \varepsilon_j \in \{-1,1\}\right\}.$$

(a) Prove that the group G with the function $d_S(g,h) = \|g^{-1}h\|_S$ becomes a metric space.

(b) Prove that every finitely generated group embeds in the group of isometries of a metric space.

Problem 1.15. Let G be a group, let $H \leq G$, and let $K \triangleleft G$. If $N \triangleleft H$, then $NK \triangleleft HK$.

Solution. Show that $NK \triangleleft H$ and $NK \triangleleft K$. ■

Definition 1.0.1. A subgroup H of a group G is called **characteristic** in G, and we denote this by $H \trianglelefteq G$, if $\varphi(H) \leq H$, for every $\varphi \in \mathrm{Aut}(G)$.

Problem 1.16. Prove that:

(a) If $H \trianglelefteq G$, then $\varphi(H) = H$, for every $\varphi \in \mathrm{Aut}(G)$.

(b) Every characteristic subgroup is normal.

(c) In contrast to normal subgroups, for characteristic subgroups transitivity holds, that is, if $H \trianglelefteq N$ and $N \trianglelefteq G$, then $H \trianglelefteq G$.

(d) If $N \trianglelefteq K$ and $K \triangleleft G$, then $N \triangleleft G$.

(e) Every subgroup of a cyclic group is characteristic.

(f) $\mathrm{C}(G) \trianglelefteq G$ and $G' \trianglelefteq G$.

(g) There exist groups for which the class of characteristic subgroups is strictly smaller than the class of normal subgroups.

Solution. (a) If $\varphi \in \mathrm{Aut}(G) \Rightarrow \varphi^{-1} \in \mathrm{Aut}(G)$, hence by applying the original definition to φ and φ^{-1}, we have that $\varphi(H) = H$.

(b) Let $g \in G$. Applying (a) to the inner automorphism τ_g, we have the desired result.

(c) Let $\varphi \in \mathrm{Aut}(G)$. Then, since N is characteristic in G, we have $\varphi(N) = N$, that is, $\varphi\big|_N \in \mathrm{Aut}(N)$. Since H is characteristic in N, we have $\varphi(H) = H$.

(d) Let $g \in G$. Then $g^{-1}Kg = K$. Thus the inner automorphism τ_g restricted to K is an automorphism of K, hence $g^{-1}Ng = \tau_g\big|_K(N) = N$, since N is characteristic in K.

(e) Let $G = \langle g \rangle$, let φ be an automorphism of G, and let $H \leq G$, that is, $H = \langle g^n \rangle$. Then $\varphi(g) = g^k$, hence $\varphi(g^n) = (g^n)^k \in H$.

(f) It is immediate that $\mathrm{C}(G), G'$ are characteristic subgroups of G.

(g) If H is a nontrivial group and $G = H \times H$ is their direct product, then $\{1\} \times H$ is normal in G, but because of the automorphism $(x, y) \mapsto (y, x)$ we observe that $\{1\} \times H$ is not characteristic.

■

Chapter 2

Group Actions

Problem 2.1. Let G be a finitely generated group whose subgroups of finite index have trivial intersection. Show that every epimorphism $\varphi\colon G \to G$ is an isomorphism.

Solution. We want to show that $K = \ker\varphi \subseteq \{1\} = \bigcap_{H \leq G,\ [G:H]<\infty} H$. Hence, it is enough to show that K is contained in every subgroup of G of finite index. Let $n \in \mathbb{N}$. Since G is finitely generated, there are only finitely many subgroups $H_1, \ldots, H_k$ of G of index n. By the correspondence theorem, there exist pairwise distinct $M_1, \ldots, M_k$ with $K \subseteq M_i$ and

$$\varphi^{-1}(H_i) = M_i \Rightarrow [G : M_i] = \left[\frac{G/K}{M_i/K}\right] = [G : H_i] = n.$$

Hence, the M_i are a rearrangement of the H_i, therefore $K \subseteq H_i$ for every i, and we have the desired result. ■

Problem 2.2. Let G be a finite group acting on a finite set X, and let $\mathrm{Fix}(g) = \{x \in X \mid g \cdot x = x\}$.

(a) Show that the number of orbits of the action is equal to $\dfrac{1}{|G|}\displaystyle\sum_{g\in G} |\mathrm{Fix}(g)|$.

(b) If the action is transitive and $|X| > 1$, then there exists an element of G that fixes no element of X.

Solution. (a) Let $A = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Then we have

$$A = \bigsqcup_{x\in X} \mathrm{Stab}_G(x) \times \{x\} = \bigsqcup_{g\in G} \{g\} \times \mathrm{Fix}(g).$$

Therefore, $\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{Stab}_G(x)|$. But, if $\mathscr{O}(x) = \mathscr{O}(y)$, it is clear that $|\text{Stab}_G(x)| = |\text{Stab}_G(y)|$. Hence, if T is a set of representatives of the orbits of the action, then

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in T} |\mathscr{O}(x)| \cdot |\text{Stab}_G(x)| = \sum_{x \in T} |G| = |T| \cdot |G|.$$

Hence, from the above relation we have the desired result.

(b) If the action is transitive, then from (a) we have that $|T| = 1$, that is, $\sum_{g \in G} |\text{Fix}(g)| = |G|$. But we have that $\text{Fix}(1) = |X| > 1$, hence

$$\sum_{g \neq 1} |\text{Fix}(g)| = G - |X| < |G|.$$

Hence, there exists $g \neq 1$ such that $\text{Fix}(g) = \emptyset$.

■

Problem 2.3. Let G be a group of order p^n, where p is prime, and let X be a finite G-set. If the prime p does not divide $|X|$, then $\bigcap_{g \in G} \text{Fix}(g) \neq \emptyset$.

Solution. We observe that

$$x \in \bigcap_{g \in G} \text{Fix}(g) \Leftrightarrow \exists x \in X : \ g \cdot x = x, \quad \forall g \in G \Leftrightarrow \exists x \in X : \ \mathscr{O}(x) = \{x\}.$$

Suppose, for contradiction, that $|\mathscr{O}(x) > 1$, for every $x \in X$. Since $|\mathscr{O}(x)| \Big| |G| = p^n$, then $p||\mathscr{O}(x)|$, for every $x \in X$. Hence, if T is a set of representatives of the orbits of the action, then $p| \sum_{x \in T} |\mathscr{O}(x) = |X|$, so we arrive at a contradiction. ■

Problem 2.4. If $|G| = n < \infty$ and p is the smallest prime divisor of n, then every subgroup H of G of index p is normal.

Solution. Consider the action of G on $X = G/H$. Then, for every $xH \in X$, we have that $|\mathscr{O}(xH)|||G|$, that is, $|\mathscr{O}(xH)| = 1$ or $|\mathscr{O}(xH)| \geq p$, since p is the smallest prime divisor of G. If T is a set of representatives of the action, then we have that

$$p = [G : H] = \sum_{xH \in T, \ x \neq H} |\mathscr{O}(xH)| + 1.$$

Hence, for every $xH \in X$, we have that $|\mathscr{O}(xH)| = 1$, that is, for every $x \in X$ we have that $H = \text{Stab}_G(xH)$, and we have the desired result. ■

Problem 2.5. Assuming as given that A_5 is simple, show that it does not contain subgroups of order $15, 20$ or 30; consequently, the converse of Lagrange's theorem does not hold.

Solution. We have that $|A_5| = 5!/2 = 60$. We distinguish cases.

- If there exists $H \leq A_5$ with $|H| = 30$, then we have that $[A_5 : H] = 2$, hence H is normal. Therefore, we arrive at a contradiction since A_5 is simple.
- If there exists $H \leq A_5$ with $|H| = 15$, then $[A_5 : H] = 4$, hence through the action of A_5 on the cosets A_5/H, a homomorphism $\varphi\colon A_5 \to \mathfrak{S}_4$ is induced. Then we have that $\ker\varphi \trianglelefteq A_5$ and $4|[A_5 : \ker\varphi]$, therefore $[A_5 : \ker\varphi] \geq 4$. Hence, since A_5 is simple, we have that $\ker\varphi = 1$. Consequently, we have that $A_5 \hookrightarrow \mathfrak{S}_4$, that is, $60|4!$. Hence, we arrive at a contradiction.
- If there exists $H \leq A_5$ with $|H| = 20$, then $[A_5 : H] = 3$. Conclude as above with a contradiction.

■

Definition 2.0.1. Let G be a group and let X, Y be G-sets. A map $\varphi\colon X \to Y$ is called a G**-map** if $\varphi(gx) = g\varphi(x)$, for every $g \in G$ and $x \in X$, and a G**-isomorphism** if φ is additionally one-to-one and onto.

Problem 2.6. Prove that G acts transitively on X if and only if X is G-isomorphic to G/H for some subgroup H of G.

Solution. If G acts transitively on X and $x \in X$, then for every $y \in X$ we have that $y = gx$, for some $g \in G$. We define $\varphi\colon X \to G/\mathrm{Stab}_G(x)$ by $gx \mapsto g\mathrm{Stab}_G(x)$. The map φ is a G-isomorphism. Conversely, if $\varphi\colon X \to G/H$, then if $\varphi(x) = H$, for every $y \in X$ we have that

$$\varphi(y) = gH = g\varphi(x) = \varphi(gx) \Rightarrow y = gx.$$

Hence, G acts transitively on X. ■

Problem 2.7. The number of subgroups of finite index n in a finitely generated group G is finite.

Solution. Let $G = \langle g_1, \ldots, g_m \rangle$. For every $H \leq G$ with $[G : H] = n < \infty$, a homomorphism $\varphi_H\colon G \to \mathfrak{S}_n$ is induced. Since every such homomorphism is completely determined by the images of the generators of G, we have only finitely many choices for such homomorphisms. It remains to show that for every $H, K \leq G$ of index n with $H \neq K$, we have $\varphi_H \neq \varphi_K$. We have, for $h \in H$, that $\varphi_H(h)(\mathrm{id}) = \mathrm{id}$ while $\varphi_K(h)(\mathrm{id}) \neq \mathrm{id}$. ■

Problem 2.8. Let G be a finitely generated group. Show that every subgroup of G of finite index contains a characteristic subgroup of finite index of G.

Solution. Let H be a subgroup of G of finite index. Then, for every $\varphi \in \mathrm{Aut}(G)$, it holds that $[G : H] = [G : \varphi(H)]$. Then, if $C = \bigcap_{\varphi \in \mathrm{Aut}(G)} \varphi(H)$, this is an intersection of finitely many groups, since G is finitely generated, whose index is finite, and it is characteristic in G. ■

Problem 2.9. Let G be a finite group and let H, K be subgroups of G. Using a suitable action, show that $|HK| \cdot |H \cap K| = |H| \cdot |K|$.

Solution.

1. *First way* (with actions): Consider the action $H \rightsquigarrow G/K$. Then we have that

   $$|\mathscr{O}(K)| = [H : \mathrm{Stab}_H(K)] = |H|/|H \cap K|$$

   and also it holds that

   $$HK = \{hk \mid h \in H, k \in K\} = \bigcup_{hK \in \mathscr{O}(K)} hK \Rightarrow |HK| = |K| \cdot |\mathscr{O}(K)|.$$

   From the above relations we have the desired result.

2. *Second way*: Consider a set of representatives $T = \{k_i H \cap K\}_i$ of the set $H \cap K$, and consider the map

   $$\varphi\colon H \times T \to HK, \quad (h, k_i H \cap K) \mapsto hk_i.$$

   Since T is a set of representatives, it is clear that φ is well-defined and one-to-one. Now, let $hk \in HK$. Then there exists $k_i H \cap K \in T$ such that $k_i H \cap K = kH \cap K$. Hence, there exists $h' \in H \cap K$ such that $k = h'k_i$. Hence, we have that $hk = \varphi(hh', k_i H \cap K)$.

■

Problem 2.10. Let G be a group, $H \leq G$, and $C_G(H) = \{g \in G \mid hg = gh,\ \forall h \in H\}$ be the centralizer of H in G. Show that $C_G(H) \trianglelefteq$

$\mathrm{N}_G(H)$ and that the quotient

$\mathrm{N}_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Solution. We have that $C_G(H) \trianglelefteq$

$\mathrm{N}_G(H)$ immediately from the definitions. For the second part of the exercise, consider the monomorphism

$$\varphi\colon \mathrm{N}_G(H)/C_G(H) \to \mathrm{Aut}(H), \quad gC_G(H) \mapsto \tau_g$$

where τ_g is the inner automorphism of H defined by g. ■

Problem 2.11. If G is a group of order p^n, where p is prime, and $1 \neq H \trianglelefteq G$, show that $H \cap \mathrm{C}(G) \neq 1$.

Solution. We want to show that $H \cap \mathrm{C}(G) \neq 1$, that is, that there exists $x \in H \setminus \{1\}$ such that $ghg^{-1} = h$, for every $g \in G$. Since H is normal, the action by conjugation of G on H is defined, and it is enough to show that there exists an orbit, other than the trivial one, which is a singleton. Indeed, if an orbit $\mathscr{O}(h)$ is not a singleton, then $|\mathscr{O}(h)| \big| |G| = p^n$, hence $p \big| |\mathscr{O}(h)|$. If T is a set of representatives of the orbits, then

$$|H| = \sum_{x \in T, x \neq 1} |\mathscr{O}(x)| + 1.$$

Since $p \big| |H|$, from the above relation it is clear that there exists $h \neq 1$ in H such that $\mathscr{O}(h) = \{h\}$. ■

Problem 2.12. Let G be a group which acts by homeomorphisms on a connected topological space X. Assume that there exists an open set U of X such that $X = \bigcup_{g \in G} gU$. Show that G is generated by the set $S = \{g \in G \mid gU \cap U \neq \emptyset\}$.

Solution. We have that $g \cdot x = f_g(x)$, where $f_g\colon X \to X$ is a homeomorphism. Consider the sets $HU, (G \setminus H)U$, where $H = \langle S \rangle$. These sets are open as unions of such sets, and $X = HU \cup (G \setminus H)U$. We have that $HU \cap (G \setminus H)U = \emptyset$. Indeed, if there exist $h \in H,\ g \in (G \setminus H)$ and $u_1, u_2 \in U$ such that $hu_1 = gu_2$, then we have that $g^{-1}hu_1 = u_2$, that is, $g^{-1}h \in H$. Thus it follows that $g \in H$, and we arrive at a contradiction. Since $HU \neq \emptyset$ and X is a connected topological space, we have that $(G \setminus H)U = 0$, that is, $G \setminus H = \emptyset$. ■

Problem 2.13. If G is a finite group and $H \leq G$, then $\left|\bigcup_{g \in G} gHg^{-1}\right| \leq |G| - [G : H] + 1$.

Solution. Let $T = \{x_1H, \ldots, x_nH\}$ be a set of representatives of G/H. Then, for $x \in \bigcup_{g\in G} gHg^{-1}$, there exist $g \in G$ and $h \in H$ such that $x = ghg^{-1}$. But $g \in G$, hence there exist x_i and $\tilde{h} \in H$ such that $g = x_i\tilde{h}$, that is, $x = x_i(\tilde{h}h\tilde{h}^{-1})x_i^{-1} \in x_iHx_i^{-1}$. Thus we conclude that

$$\bigcup_{g\in G} gHg^{-1} = \bigcup_{x_iH\in T} x_iHx_i^{-1}.$$

Thus we have that

$$\left|\bigcup_{g\in G} gHg^{-1}\right| = \left|\bigcup_{x_iH\in T} x_iHx_i^{-1}\right| \leq \sum_{x_iH\in T} \left|x_iHx_i^{-1} \setminus \{1\}\right| + 1 = [G : H]\cdot(|H| - 1) + 1 = |G| - [G : H] + 1.$$

■

Problem 2.14. (a) Let G be a finite group and $H \subsetneqq G$. Show that there exists an element of G which is not contained in the union of the conjugates of H.

(b) If G is finite and all its maximal subgroups are conjugate, then G is cyclic.

Solution. (a) The desired result follows immediately from Exercise 2.13.

(b) If G has no proper nontrivial subgroups, then it is clear that it is cyclic. Otherwise, let H be a maximal proper subgroup of G. Since every maximal subgroup of G is conjugate to H, then by (a) there exists $g \in G$ which is not contained in any maximal subgroup of G. Thus we conclude that $G = \langle g\rangle$.

■

Problem 2.15. If H is a proper subgroup of finite index in a group G, then the union of the conjugates $\bigcup_{g\in G} gHg^{-1}$ of H is properly contained in G.

Solution. Suppose, for contradiction, that $G = \bigcup_{g\in G} gHg^{-1}$. Consider the action of G on the cosets G/H. From the usual induced homomorphism φ, there exists $K = \ker\varphi \lhd G$ with $K \subseteq H$ and $[G : K] < \infty$. Since H is a proper subgroup of G, then $H/K \subsetneqq G/K$, and moreover $G/K = \bigcup_{g\in G} g(H/K)g^{-1}$. Since G/K is finite, we arrive at a contradiction by Exercise 2.13. ■

Chapter 3

Sylow Theorems

Problem 3.1. Let G be a finite p-group and let H be a maximal proper subgroup of G. Then $H \lhd G$ and $[G : H] = p$.

Solution. Since G is a p-group and $H \subsetneqq G$, the normalizer condition is satisfied, that is, $H \subsetneqq$

$\mathrm{N}_G(H)$. Since H is maximal, we have

$\mathrm{N}_G(H) = G$. From Sylow's theorem and the correspondence theorem, it is immediate that $[G : H] = p$. ■

Problem 3.2. Let G be a periodic group, that is, every element has finite order, and let Π be the set of prime divisors of the orders of the elements of the group. If for every $p \in \Pi$ there exists a unique Sylow p-subgroup G_p, then G is the direct product of the G_p, $p \in \Pi$.

Solution. First we will show that every G_p is normal. Let $g \in G$. Then gG_pg^{-1} is a p-group, so it is contained in a Sylow p-subgroup of G. Thus we have $gG_pg^{-1} \subseteq G_p$. By the maximality of G_p, we have $gG_pg^{-1} = G_p$. Now it is clear that any two Sylow subgroups G_p, G_q with $p \neq q$ have trivial intersection. It remains to show that $G = \langle G_p \mid p \in \Pi \rangle$. Let $g \in G$. We have $o(g) = p_1^{n_1} \cdots p_k^{n_k}$. We have $\langle g \rangle = \langle g_1 \rangle \cdot \langle g_2 \rangle \cdots \langle g_k \rangle$, where $g_i \in \langle g \rangle$ with $o(g_i) = p_i^{n_i}$. Thus we have $\langle g_i \rangle \subseteq G_{p_i}$, therefore

$$g \in \langle g \rangle \subseteq G_{p_1} \cdots G_{p_k} \subseteq \langle G_p \mid p \in \Pi \rangle.$$

■

Problem 3.3. (a) Let G be a group, let K be a finite normal subgroup of G, and let P be a Sylow p-subgroup of K. Show that $G =$

$\mathrm{N}_G(P)K$.

(b) If every maximal subgroup of a finite group G is normal in G, then every Sylow subgroup of G is normal.

Solution. (a) Since $P \subseteq K$ and K is normal, for every $g \in G$ we have $gPg^{-1} \subseteq K$. Let $g \in G$. Then gPg^{-1} is a Sylow subgroup of K, therefore there exists $x \in K$ such that $gPg^{-1} = xPx^{-1}$, that is,

$$g^{-1}x \in \mathrm{N}_G(P) \Rightarrow g^{-1} \in \mathrm{N}_G(P)K \Rightarrow g \in \mathrm{N}_G(P)K.$$

(b) Let P be a Sylow p-subgroup of G. Suppose, for contradiction, that

$\mathrm{N}_G(P) \subsetneqq G$, that is, there exists a maximal subgroup M of G such that

$$P \subseteq \mathrm{N}_G(P) \subseteq M \subsetneqq G.$$

By the initial hypothesis, M is normal, hence for every $g \in G$ we have $gPg^{-1} \subseteq M$, that is, $gPg^{-1} \in \mathrm{Syl}_p(M)$, for every $g \in G$. Let $g \in G$. Then there exists $x \in M$ such that $gPg^{-1} = xPx^{-1}$, that is, $x^{-1}g \in$

$\mathrm{N}_G(P) \subseteq M$. Hence $g \in M$, and since g was arbitrary, we arrive at a contradiction.

■

Problem 3.4. Let G be a finite group and let P be a Sylow p-subgroup of G.

(a) If

$\mathrm{N}_G(P) \leq H \leq G$, then $[G : H] \equiv 1 \mod p$.

(b) If $K \lhd G$, then $K \cap P$ is a Sylow p-subgroup of K and PK/K is a Sylow p-subgroup of G/K.

(c) If $K \lhd G$, then $n_p(G/K) \leq n_p(G)$, where n_p denotes the number of Sylow p-subgroups.

Solution. (a) Let T be a set of representatives of G/H. Define the map

$$\varphi\colon T \to \mathrm{Syl}_p(G), \quad xH \mapsto xPx^{-1}.$$

The map φ is onto and one-to-one, since $xPx^{-1} = x'Px^{-1} \Rightarrow x^{-1}x' \in$

$\mathrm{N}_G(P) \subseteq H$. Hence, we have

$$[G : H] = |T| = n_p(G) \equiv 1 \mod p.$$

(b) Let Q be a Sylow p-subgroup of K. Then, for some $g \in G$, it can be written in the form

$$Q = K \cap \left(gPg^{-1}\right) = g\,(K \cap P)\,g^{-1} \Rightarrow |Q| = |K \cap P|.$$

From the last relation we have the desired result.

Now, $|PK/K| = |P : K \cap P|$, hence PK/K is a p-subgroup of G/K with

$$p \not| \, |G/K : PK/K| = |G : PK|,$$

hence it is a Sylow p-subgroup of G/K.

(c) If Q is a Sylow p-subgroup of G/K, then from (b) it is of the form

$$Q = gK\,(PK/K)\,g^{-1}K = (gPKg^{-1})/K = \left(gPg^{-1}\right)K/K,$$

where the last equality follows from the normality of K. Hence every Sylow p-subgroup of G/K is of the form $P'K/K$, where P' is a Sylow p-subgroup of G. Thus it is clear that $n_p(G/K) \leq n_p(G)$.

■

Problem 3.5. Let D_n be the dihedral group of order $2n$. Show that if n is odd, then all Sylow subgroups of D_n are cyclic. Does the conclusion hold if n is even?

Solution. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be odd. If R_n is the group of rotations of D_n, we know that it is cyclic of order n. If $P \in \mathrm{Syl}_{p_i}(G)$, then it is conjugate to a Sylow p_i-subgroup of R_n, that is, $P = x\langle g\rangle x^{-1} = \langle xgx^{-1}\rangle$.

If $n = 4$, then $|\mathbf{D}_4| = 2^3$, but it is not cyclic, since $\mathbf{D}_4$ is not abelian. ■

Problem 3.6. Let $P_1, \ldots, P_m$ be the Sylow p-subgroups of a finite group G, and let S_P be the permutation group of the set $\{P_1, \ldots, P_m\}$. We define a map $\varphi\colon G \to S_P$ such that $\varphi(g)$ is the permutation $P_i \mapsto gP_ig^{-1}$.

(a) Show that φ is a homomorphism and find its kernel.

(b) Show that the dihedral group D_n is isomorphic to a subgroup of $\mathfrak{S}_n$ if n is odd.

Solution. (a) It is immediate that φ is a homomorphism. Show that $\ker\varphi = \bigcap_{i=1}^{m}$

$N_G(P_i)$.

(b) Let $P = \langle a\rangle$ be a Sylow 2-subgroup of D_n. Consider the action of D_n on the cosets of D_n/P, which induces a homomorphism $\varphi\colon D_n \to \mathfrak{S}_n$. It is enough to show that $\ker\varphi = 1$. We know that $\ker\varphi \subseteq P$ and moreover

$$\ker\varphi = \bigcap_{g\in D_n} g^{-1}Pg = \bigcap_{g\in D_n} \langle g^{-1}ag\rangle.$$

If $\ker\varphi \neq 1$, then there exists $h \in \ker\varphi$ with $h = g^{-1}ag = a$, for every $g \in D_n$. Hence, $P \subseteq Z(D_n)$. If $\mathrm{Rot}_n = \langle r\rangle$, then since $D_n = \langle r, a\rangle$, from the previous relation it follows that D_n is abelian, and we arrive at a contradiction. Hence, $\ker\varphi = 1$, and we have the desired result.

■

Problem 3.7. Let G be a finite group with order $|G| = 2n$, where n is odd. Then there exists a normal subgroup N of G with $|N| = n$. In particular, G is not simple.

Solution. Suppose that $n = p_1^{a_1}\cdots p_n^{a_k}$. Then there exist $P_i \in \mathrm{Syl}_{p_i}(G)$, and it follows that $|N| = n$, where $N = P_1\cdots P_k$. Consider the action of G on the cosets of G/N. Then a monomorphism $G/K \hookrightarrow S_2$ is induced, where $K \subseteq N$ is the kernel of the corresponding homomorphism induced by the action. Therefore $|G/K| = 1$ or 2, and since $N \neq G$, then $G/K = 2$ and $N = K$, that is, $N \lhd G$. ■

Problem 3.8. If G is a finite group of order pq, where p and q are primes with $p \leq q$, then G has a normal subgroup of order q and hence cyclic. In particular, G is not simple.

Solution. We have that $n_q \equiv 1 \mod q$ and $n_q|p$. If $n_q = p$, then $q|p-1$, and we arrive at a contradiction. Consequently, $n_q = 1$, hence G has a unique normal Sylow q-subgroup. ■

Problem 3.9. Classify the groups of order $2p$, where p is an odd prime.

Solution. ■

Problem 3.10. A finite group of order p^2q, where p and q are primes, is not simple.

Solution. Let G be a group with order $|G| = p^2q$, where p and q are primes.

- Obviously, if $p = q$, then G is not simple, since it has nontrivial center.
- Otherwise, if $q < p$, the desired result is proved similarly to Exercise 3.8.
- If $p < q$, we have that $n_p = 1$ or q. If $n_p = 1$, then we have the desired result. If $n_p = q$, then we distinguish cases:
  (a) If any two Sylow p-subgroups have trivial intersection, then we have $q(p^2 - 1)$ elements of order a power of p, hence there exists a unique Sylow q-subgroup of G.
  (b) If there exist different Sylow p-subgroups P, Q of G with $P \cap Q \neq \{1\}$, then it holds that $P, Q \subsetneqq$

  $N_G(P \cap Q)$, hence $G =$

  $N_G(P \cap Q)$. Consequently, $P \cap Q$ is normal in G.

■

Problem 3.11. If G is a simple group of order 60, then $G \cong A_5$.

Solution. We have that $|G| = 2^2 \cdot 3 \cdot 5$. If n_p is the number of Sylow p-subgroups of G, as is known, we have that $n_5 = 6$ and $n_3 = 4$ or 10. Hence, the number of elements of order 5 is equal to $6 \cdot (5 - 1) = 24$, and the number of elements of order 3 is between $4 \cdot (3 - 1) = 12$ and $10 \cdot (3 - 1) = 20$. Thus, the number of elements of order 3 or 5 is between 36 and 44. Now, since G is simple, and by the previous observation, we have that $n_2 = 15$. We distinguish cases:

- If any two different Sylow 2-subgroups of G have trivial intersection, then there are $(2^2 - 1) \cdot 15 = 45$ elements of order 2 or 2^2, and from the above observation we arrive at a contradiction.
- Hence, there exist $P, Q \in \mathrm{Syl}_2(G)$ with $P \neq Q$ and $1 \neq P \cap Q$. Then, if $N =$

  $N_G(P \cap Q)$, we have $P, Q \subsetneqq N$, since P, Q are abelian and different from each other. Hence, we have that $|N| = 2^2 \cdot 5$ or $|N| = 2^2 \cdot 3$ or $|N| = |G|$.

(a) If $|N| = 2^2 \cdot 3$, then $[G : N] = 3$, and from the action of G on the cosets of G/N, a homomorphism $\varphi\colon G \to \mathfrak{S}_3$ is induced with $\ker\varphi \lhd G$ and $\ker\varphi \subseteq N$. Therefore, we have $\ker\varphi = \{1\}$ and $G \hookrightarrow \mathfrak{S}_3$, a contradiction.

(b) If $|N| = |G|$, then $N = G$, therefore $1 \neq P \cap Q \lhd G$, a contradiction.

(c) Hence, the only possible case is $|N| = 3^2 \cdot 2$. Consider the action of G on the cosets of G/N. Then a homomorphism $\varphi\colon G \to \mathfrak{S}_5$ is induced. Since $\ker\varphi \trianglelefteq G$ and $\ker\varphi \subseteq N$, then $\ker\varphi = \{1\}$, hence $G \hookrightarrow \mathfrak{S}_5$. Since the unique simple subgroup of order 60 of $\mathfrak{S}_5$ is A_5, we have $G \cong \mathrm{Im}\varphi = A_5$.

■

Problem 3.12. Show that there are no simple groups of orders $90, 132, 144, 150$.

Solution. 1. Let G be a simple group of order $|G| = 90 = 2 \cdot 3^2 \cdot 5$. By known computations, we conclude that $n_5 = 6$ and $n_3 = 10$. Hence, $(5-1) \cdot 6 = 24$ elements have order 5. We distinguish cases:

- If any two different Sylow 3-subgroups of G have trivial intersection, then there are $10 \cdot (3^2 - 1) = 80$ elements of order 3 or 3^2, where we arrive at a contradiction from the initial hypothesis.
- Suppose that there exist $P, Q \in \mathrm{Syl}_3(G)$ with $P \neq Q$ and $1 \neq P \cap Q$. Then, if $N =$

  $N_G(P \cap Q)$, we have $P, Q \subsetneqq N$, since P, Q are abelian and different from each other. Hence, $|N| = 3^2 \cdot 5$ or $|N| = 3^2 \cdot 2$ or $|N| = |G|$.

  (a) If $|N| = 3^2 \cdot 5$, then $[G : N] = 2$, hence $1 \neq N$ is normal in G, a contradiction.

  (b) If $|N| = 3^2 \cdot 2$, then similarly to the above exercise, G embeds in $\mathfrak{S}_5$, while $|G| = 90 \nmid 5!$, a contradiction.

  (c) If $|N| = |G|$, then $N = G$ and $1 \neq P \cap Q$ is normal in G, a contradiction.

2. Suppose that there exists a simple group G with $|G| = 132 = 2^2 \cdot 3 \cdot 11$. By the usual computations, it holds that $n_{11} = 12$, that is, there are $12 \cdot (11-1) = 120$ elements of order 11. Now, since G is simple, we have $n_3 = 4$ or 22. We distinguish cases:

   - If $n_3 = 4$, there are $4 \cdot (3-1) = 8$ elements of order 3. Hence, we conclude that there exists a unique Sylow 2-subgroup of G, that is, a normal one, a contradiction.
   - If $n_3 = 22$, there are $22 \cdot (3-1) = 44$ elements of order 3. Hence, the number of elements of order 3 or 11 is $44 + 120 = 165 > |G|$, a contradiction.

3. Suppose that there exists a simple group G with $|G| = 144 = 2^4 \cdot 3^2$. We have that $n_3 = 4$ or 16. We distinguish cases:

- Suppose that $n_3 = 4$. If $P \in \mathrm{Syl}_3(G)$, then we have $n_3 = [G :$

  $N_G(P)]$, that is, we conclude that G embeds in $\mathfrak{S}_4$ (why?), a contradiction.
- If $n_3 = 16$, we distinguish the following cases:
  (a) If any two Sylow 3-subgroups have trivial intersection, then there are $16\cdot(3^2-1) = 128$ elements, that is, there exists a unique Sylow 2-subgroup of G, a contradiction.
  (b) Suppose that there exist $P, Q \in \mathrm{Syl}_3(G)$ with $P \neq Q$ and $1 \neq P \cap Q$. Then, if $N =$

  $N_G(P \cap Q)$, we have $P, Q \subsetneqq N$, since P, Q are abelian and different from each other. Hence, we have that $|N| = 3^2 \cdot 2^i$ with $i = 1, \ldots, 4$. We distinguish cases:
     i. If $|N| = 3^2 \cdot 2$, then $[N : P] = [N : Q] = 2$, that is, P, Q are normal in N. Since P, Q are Sylow 3-subgroups of N and are moreover normal, we have $P = Q$, a contradiction.
     ii. If $|N| = 3^2 \cdot 2^2$, then $G \hookrightarrow \mathfrak{S}_4$ (why?), a contradiction.
     iii. If $|N| = 3^2 \cdot 2^3$, then $[G : N] = 2$, consequently $1 \neq N$ is normal in G, a contradiction.
     iv. If $|N| = 3^2 \cdot 2^4$, then $N = G$, therefore $1 \neq P \cap Q$ is normal in G, a contradiction.

4. Similarly to the previous cases.

■

The purpose of the next exercises is to give a different proof of Sylow's theorem.

Problem 3.13. Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is prime, be the field with p elements, let $\mathrm{GL}_n(\mathbb{F}_p)$ be the group of invertible $n \times n$ matrices over $\mathbb{F}_p$, and let $\mathrm{UT}_n(\mathbb{F}_p)$ be its subgroup consisting of those matrices whose entries below the main diagonal are zero and whose every entry on the main diagonal is equal to 1. That is, every matrix in $\mathrm{UT}_n(\mathbb{F}_p)$ has the following form:

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Show that $\mathrm{UT}_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

Solution. First, we observe that $A \in \mathrm{GL}_n(\mathbb{F}_p)$ if and only if A has linearly independent columns, and from this fact we have that

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots \left(p^n - p^{n-1}\right) = p \cdot p^2 \cdots p^{n-1} \cdot m = p^{n(n-1)/2} m$$

with $\left(p^{n(n-1)/2}, m\right) = 1$. Now, it is clear that $|\mathrm{UT}_n(\mathbb{F}_p)| = p \cdot p^2 \cdots p^{n-1} = p^{n(n-1)/2}$, that is, $\mathrm{UT}_n(\mathbb{F}_p)$ is a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$. ∎

Problem 3.14. Let H be a Sylow p-subgroup of a finite group G, and let K be a subgroup of G whose order is a multiple of p. Show that there exists $x \in G$ such that $K \cap xHx^{-1}$ is a Sylow p-subgroup of K.

Solution. Let P be a Sylow p-subgroup of the finite group K. Then, as a p-group of G, it is contained in some Sylow p-subgroup of G, that is, there exists $x \in G$ such that $P \subseteq xHx^{-1}$. Therefore, $P \subseteq K \cap xHx^{-1}$, where $K \cap xHx^{-1}$ is a p-group of K. Hence, we have that $P = K \cap xHx^{-1}$. ∎

Problem 3.15. Let G be a group of order $p^k m$, where p is a prime that does not divide m. Then there exists at least one Sylow p-subgroup of G.

Solution. We know that G embeds in $\mathrm{GL}_n(\mathbb{F}_p)$ through some φ, where $n = |G|$. Hence, there exists a subgroup H of $\mathrm{GL}_n(\mathbb{F}_p)$ whose order is a multiple of p. From Exercises 3.11 and 3.12, we have that there exists $A \in \mathrm{GL}_n(\mathbb{F}_p)$ such that $P = H \cap A\left(\mathrm{UT}_n(\mathbb{F}_p)\right)A^{-1} \in \mathrm{Syl}_p(H)$. Therefore, we have that $\varphi^{-1}(P) \in \mathrm{Syl}_p(G)$. ∎

Chapter 4

Direct Products

Problem 4.1. (a) Let a, b be two elements of finite order of a group G. If a, b commute and the orders $o(a)$ and $o(b)$ are relatively prime, then $o(ab) = o(a) \cdot o(b)$.

(b) Show that the multiplicative group F^* of a finite field F is cyclic.

Solution. (a) Let $o(a) = m,\ o(b) = n$, and $o(ab) = k$. Then $(ab)^{mn} = a^{mn}b^{mn} = 1$, hence $k|mn$. It remains to show that $mn|k$, and since $(m, n) = 1$, it is enough to show that $m|k$ and $n|k$. We have

$$(ab)^k = a^k b^k = 1 \Rightarrow a^k = b^{-k}.$$

Since

$$o\left(a^k\right) = o\left(b^{-k}\right)|n \quad \text{and} \quad o\left(a^k\right)|m \quad \Rightarrow o\left(a^k\right) = 1,$$

we have $a^k = b^{-k} = 1$, and we have the desired result.

(b) Let $|F^*| = p^n - 1 = p_1^{a_1} \cdots p_k^{a_k}$, where the p_i are distinct primes. By the fundamental structure theorem for abelian groups, we have

$$F^* \cong A_1 \times \cdots \times A_k,$$

where $|A_i| = p_i^{a_i}$, and every $A \in \{A_1, \ldots, A_k\}$ is of the form

$$A = \mathbb{Z}_{p^{\beta_1}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$$

with $\beta_1 + \cdots + \beta_t = a$. If we suppose, for contradiction, that there exists such an A with some $\beta_i < a$, then by (a), every element of F^* would have order dividing some $\ell < p^n - 1$. Then the polynomial $x^\ell - 1$ would have $p^n - 1 > \ell$ roots, so we arrive at a contradiction. Hence,

$$F^* \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} \cong \mathbb{Z}_{p^n-1}.$$

■

Problem 4.2. (a) If $M \triangleleft G$ and $N \triangleleft K$, show that $M \times N \triangleleft G \times K$ and $(G \times K)/(M \times N) \cong G/M \times K/N$. Generalize this for a finite number of factors.

(b) Show that if $H, K \triangleleft G$ and $G = HK$, then $G/(H \cap K) \cong (H/H \cap K) \times (K/H \cap K)$.

(c) If $H, K \triangleleft G$, show that $G/(H \cap K)$ is isomorphic to a subgroup of $G/H \times G/K$.

Solution. (a) Consider the map $\varphi\colon G \times K \to G/M \times K/N$ given by $\varphi(g, k) = (gM, kN)$. The map φ is an epimorphism with $\ker \varphi = M \times N \triangleleft G \times K$, hence by the first isomorphism theorem we have the desired result.

(b) Immediate from the definition of the direct product.

(c) Consider the map $\varphi\colon G/(H \cap K) \to G/K \times G/H$ given by $\varphi(g(H \cap K)) = (gH, gK)$, and show that it is a monomorphism of groups.

■

Problem 4.3. Let $G = H_1 \times \cdots \times H_n$. Show that $\mathrm{C}(G) = \mathrm{C}(H_1) \times \cdots \times \mathrm{C}(H_n)$.

Solution. We will prove one inclusion indicatively. Let $g = (g_1, \ldots, g_n) \in \mathrm{C}(G)$ and let $x_i \in H_i$. Then we have

$$(g_1, \ldots, g_n) \cdot (x_1, \ldots, x_n) = (x_1, \ldots, x_n) \cdot (g_1, \ldots, g_n) \Leftrightarrow (g_1x_1, \ldots, g_nx_n) = (x_1g_1, \ldots, x_ng_n).$$

Thus it is clear that $g_ix_i = x_ig_i$, for every i and arbitrary $x_i \in H_i$. Hence, we have $g_i \in \mathrm{C}(H_i)$. ■

Problem 4.4. If G is finite abelian and $|G| = n$, then for every divisor m of n, the group G contains a subgroup of order m.

Solution. Let $n = p_1^{a_1} \cdots p_n^{a_n}$, where the p_i are distinct primes. The group G is written as a direct product of its Sylow subgroups, $G = P_1 \times \cdots \times P_n$, where each such factor P_i is of the form $\mathbb{Z}_{p_i^{b_1}} \times \cdots \times \mathbb{Z}_{p_i^{b_t}}$ with $b_1 + \cdots + b_t = a_i$. Let $m|n$, that is, $m = p_1^{c_1} \cdots p_n^{c_n}$ with $c_i \leq a_i$. For every i, there exists a subgroup Q_i of P_i of order $p_i^{c_i}$ (why?). Then $H = Q_1 \times \cdots \times Q_n$ is a subgroup of G of order m. ■

Problem 4.5. (a) How many abelian groups are there, up to isomorphism, of order 231 or 432?

(b) Given that there are 14 groups, up to isomorphism, of order 81, find the number of groups, up to isomorphism, of order 891.

Solution. Let G be abelian of order $n = p_1^{a_1} \cdots p_n^{a_n}$. Then G is written as a direct product of its Sylow subgroups, $G = P_1 \times \cdots \times P_n$, where each such factor P_i is of the form $\mathbb{Z}_{p_i^{b_1}} \times \cdots \times \mathbb{Z}_{p_i^{b_t}}$ with $b_1 + \cdots + b_t = a_i$.

(a)
- Let G be abelian of order $231 = 3 \cdot 7 \cdot 11$. Hence, there is a unique such G, namely $\mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$.
- Let G be abelian of order $432 = 2^4 \cdot 3^3$. From the initial observation, since there are 14 non-isomorphic abelian groups of order 2^4 and 4 non-isomorphic abelian groups of order 3^3, there are $14 \cdot 4 = 56$ non-isomorphic abelian groups of order 432.

(b) Let G be an abelian group of order $891 = 81 \cdot 11$. From the initial observation and the hypothesis, there are $14 \cdot 1 = 14$ non-isomorphic abelian groups of order 891.

■

Problem 4.6. (a) Show that the set of elements of finite order of an abelian group G is a subgroup of G, denoted by $T(G)$, and that every nontrivial element of $G/T(G)$ has infinite order.

(b) Let G and H be abelian groups. Then $T(G) \cong T(H)$ and $G/T(G) \cong H/T(H)$.

Solution. (a) Immediate by applying the definitions, since for every $a, b \in G$ we have $(ab)^n = a^n b^n$.

(b) Since $G \cong H$, there exists an isomorphism $\varphi\colon G \to H$. Show that the restriction of φ to $T(G)$ is an isomorphism from $T(G)$ to $T(H)$. Now, let $\pi\colon H \to H/T(H)$ be the natural projection. The composition $\psi = \pi \circ \varphi\colon G \to H/T(H)$ is an epimorphism of groups with $\ker \psi = T(G)$. By the first isomorphism theorem we have the desired result.

■

Problem 4.7. For an abelian group G and every positive integer n, we define, using additive notation, $nG = \{ng \mid g \in G\}$ and $G[n] = \{g \in G \mid ng = 0\}$. Show the following:

(a) nG and $G[n]$ are subgroups of G.

(b) If G and H are abelian, then $n(G \times H) \cong nG \times nH$ and $(G \times H)[n] = G[n] \times H[n]$.

(c) $n\mathbb{Z}_m \cong \mathbb{Z}_k$, where $k = \frac{m}{(m,n)}$, and $\mathbb{Z}_m[n] = \mathbb{Z}_{(m,n)}$.

(d) If G is finite abelian and q is a prime that does not divide $|G|$, then $qG = G$.

(e) If G is a finite abelian p-group, then $G[p]$ is a finite-dimensional vector space over $\mathbb{Z}_p$.

(f) If $G = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_r}}$, where p is prime, then $pG = \mathbb{Z}_{p^{m_1 - 1}} \times \cdots \times \mathbb{Z}_{p^{m_r - 1}}$.

Solution. (a) Immediate.

(b) Immediate.

(c) We have $k(n[1]) = [kn] = 0$. Hence, $o([n])|k$. Now, let λ be such that $\lambda[n] = [\lambda n] = 0$, that is, $m|\lambda n$. Therefore, there exists μ such that $\lambda n = \mu m \Rightarrow \lambda n = xk$. Since $(n, k) = 1$, we have $k|\lambda$, hence $k \leq \lambda$. Thus $n\mathbb{Z}_m = \langle n[1] \rangle$ is cyclic of order k. Now, it is clear that $[k] \in \mathbb{Z}_m[n]$, and show that if $[x] \in \mathbb{Z}_m[n]$, then $k|x$, that is, $\mathbb{Z}_m[n] = \langle [k] \rangle$. Now, since $o([k]) = (m, n)$, we have the desired result.

(d) Let $g \in G$. Since $(q, |G|) = 1$, there exist $x, y \in \mathbb{Z}$ such that $1 = xq + y|G|$. Hence, we have $g = q(xg) \in qG$.

(e) The group $G[p]$ is an abelian group with respect to $(+)$. Consider the action of $\mathbb{Z}_p$ on $G[p]$ as follows: $([x], g) \mapsto x \cdot g$. This action is well-defined, since if $[x] = [y]$, then $p|x - y$, therefore if $g \in G[p]$, we have $(x - y)g = 0$, hence $[x] \cdot g = [y] \cdot g$. It is immediate that with the above scalar multiplication, $G[p]$ obtains the structure of a $\mathbb{Z}_p$-vector space.

(f) From (b), we have

$$pG = p\mathbb{Z}_{p^{m_1}} \times \cdots \times p\mathbb{Z}_{p^{m_r}}.$$

From (c), it is immediate that $p\mathbb{Z}_{p^{m_i}} \cong \mathbb{Z}_{p^{m_i - 1}}$, hence we have the desired result.

■

Chapter 5

Semidirect Products

Problem 5.1. A cyclic group of order p^2, where p is prime, cannot be decomposed as a semidirect product.

Solution. Let G be a cyclic group of order p^2. Suppose, for contradiction, that there exist nontrivial cyclic subgroups $N, H \neq G$ such that $G = N \rtimes H$. Then we know that N, H are cyclic of order p, and moreover, since there is a unique subgroup of G of order p, we have $H = N$. This is a contradiction, since $G = N \rtimes H$, hence $H \cap N = \{1\}$. ■

Problem 5.2. Every group G of order pq, where p, q are distinct primes, is a semidirect product of cyclic subgroups of orders p and q, respectively.

Solution. Suppose that $p < q$. If n_q is the number of Sylow q-subgroups of G, then $n_q | p$, hence $n_q = 1$ or p, and $n_q \equiv 1 \mod q$. Since $p < q$, it is clear that $n_q = 1$, hence there exists a unique and normal Sylow q-subgroup Q of G, which is obviously cyclic of order q. If $P \in \mathrm{Syl}_p(G)$, cyclic of order p, then $P \cap Q = \{1\}$. Therefore, $|QP| = |Q| \cdot |P|/|P \cap Q| = pq = |G|$, hence $G = QP$. Thus G is a semidirect product of cyclic subgroups of orders p and q, respectively. ■

Problem 5.3. If $G = N \rtimes H$, then $G/N \cong H$.

Solution. Consider the homomorphism $\varphi\colon G/N \to H$, where $nhN \mapsto h$. ■

Problem 5.4. The group $G = N \rtimes_\varphi H$ is not abelian if φ is not trivial.

Solution. If φ is not trivial, then there exists $h \in H$ such that $\varphi(h) \neq \mathrm{id}_H$. That is, there exists $n \in N$ such that $\varphi(h)(n) \neq n$. Show that $(n, 1) \cdot (1, h) \neq (1, h) \cdot (n, 1)$. ■

Problem 5.5. For the group $G = N \rtimes_\varphi H$, the kernel $\ker\varphi$ consists of the elements of $\tilde{H}$ that commute with every element of the subgroup $\tilde{N}$. That is, $(1, \ker\varphi) = C_{\tilde{H}}(\tilde{N})$.

Solution. The desired result follows immediately by applying the definitions. ■

Problem 5.6. Every group G that decomposes as a semidirect product $G = N \rtimes_\varphi H$, where N, H are cyclic of orders 10 and 3, respectively, is cyclic.

Solution. It is enough to show that φ is trivial, since then

$$G = N \rtimes_\varphi H = N \times H \cong \mathbb{Z}_{10} \times \mathbb{Z}_3 \cong \mathbb{Z}_{30}.$$

We have

$$\mathrm{Aut}(\mathbb{Z}_{10}) \cong \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_5) \cong \mathrm{Aut}(\mathbb{Z}_2) \times \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4.$$

Then $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_{10}) = \mathbb{Z}_4$. If $\ker\varphi \neq \mathbb{Z}_3$, then $\ker(\varphi) = 1$, that is, $\mathbb{Z}_3 \hookrightarrow \mathbb{Z}_4$, and we arrive at a contradiction. Consequently, $\ker\varphi = \mathbb{Z}_3$, that is, φ is trivial. ■

Problem 5.7. For every prime p, construct a non-abelian group of order p^3.

Solution. Let $N = \mathbb{Z}_p \times \mathbb{Z}_p = \langle a \rangle \times \langle b \rangle$. Define a map

$$\varphi\colon N \to N, \quad \varphi\left(a^k b^s\right) = a^k b^{k+s},\ 0 \leq k,\ s < p,$$

which is an automorphism. For every $n = 0, \ldots, p-1$, we have that $\varphi^n\left(a^k b^s\right) = a^k b^{nk+s}$ is an automorphism, and φ has order p. Define a map

$$\psi\colon \mathbb{Z}_p \to \mathrm{Aut}(N), \quad [a] \mapsto \varphi^a,$$

which is a nontrivial group homomorphism. Thus the semidirect product $G = N \rtimes_\psi \mathbb{Z}_p$ is defined, and by Exercise 5.4 it is a non-abelian group of order p^3. ■

Problem 5.8. Let K, H be two groups, let $\varphi\colon K \to \mathrm{Aut}(H)$, and let $\sigma \in \mathrm{Aut}(K)$. Prove that the map $\psi\colon H \rtimes_{\varphi\circ\sigma} K \to H \rtimes_\varphi K$ given by $\psi(h, k) = (h, \sigma(k))$ is a group isomorphism.

Solution. The map ψ is a homomorphism. Indeed, if $(h_1, k_1), (h_2, k_2) \in H \rtimes_{\varphi\circ\sigma} K$, then

$$\begin{aligned}
& \psi\left((h_1, k_1) \cdot (h_2, k_2)\right) = \psi(h_1(\varphi\circ\sigma)(k_1)(h_2), k_1 k_2) \\
= \ & (h_1\varphi(\sigma(k_1))(h_2), \sigma(k_1 k_2)) \\
= \ & (h_1\varphi(\sigma(k_1))(h_2), \sigma(k_1)\sigma(k_2)) \\
= \ & \psi(h_1, k_1) \cdot \psi(h_2, k_2).
\end{aligned}$$

Now it is immediate that ψ is one-to-one and onto. ■

Problem 5.9. Let K be a cyclic group, let H be an arbitrary group, and let $\varphi_1, \varphi_2 \colon K \to \mathrm{Aut}(H)$ be homomorphisms such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite, assume additionally that the homomorphisms φ_1, φ_2 are one-to-one. Show that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

Solution. ■

Problem 5.10. Let p and q be primes with $p > q$.

(a) If $p \not\equiv 1 \mod q$, then every group of order pq is cyclic.

(b) If $p \equiv 1 \mod q$, there are two groups of order pq, up to isomorphism: the cyclic group $\mathbb{Z}_{pq}$ and a non-abelian group $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$.

Solution. Initially, let n_p be the number of Sylow p-subgroups of G. Then $n_p | q$, that is, $n_p = 1$ or q, and $n_p \equiv 1 \mod p$. Therefore, it is clear that $n_p = 1$, that is, there exists a unique Sylow p-subgroup of G, say P, which is cyclic of order p.

(a) We have $n_q | p$ and $n_q \equiv 1 \mod q$. Since $p \not\equiv 1 \mod q$, it is clear that $n_q = 1$. Thus, if Q is the unique Sylow q-subgroup of G, then it is normal. Therefore, $G = P \times Q \cong \mathbb{Z}_{pq}$.

(b) If $Q \in \mathrm{Syl}_q(G)$, then $G = P \rtimes Q \cong \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$.

- If φ is the trivial homomorphism, then $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ is the corresponding direct product, that is, the cyclic group of order pq.
- If $\varphi \colon \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_{p-1}$ is nontrivial, then $\ker \varphi \neq \mathbb{Z}_q$, hence $\ker(\varphi) = 1$, that is, $\mathrm{im}\varphi$ is the unique cyclic subgroup of $\mathbb{Z}_{p-1}$ of order q, which exists because $q | p - 1$. Now, if $a \in \mathbb{Z}_q$ and $b \in \mathbb{Z}_{p-1}$ are generators, define $\varphi \colon \mathbb{Z}_q \to \mathbb{Z}_{p-1}$ by $\varphi(a) = b^{\frac{p-1}{q}}$. Since φ is not trivial, $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ is not abelian. By the above observation and Exercise 5.9, for every other nontrivial homomorphism $\psi \colon \mathbb{Z}_q \to \mathbb{Z}_{p-1}$, we have

$$\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_\psi \mathbb{Z}_q.$$

■

Problem 5.11. Find the smallest odd n for which there exists a non-abelian group of order n.

Solution. From Exercise 5.10, since $21 = 3 \cdot 7$ and $7 \equiv 1 \mod 3$, we have $n = 21$. ■

Problem 5.12. Show that there are exactly 5 groups of order 12, up to isomorphism, of which three are non-abelian.

Solution. We have $n_3 = 1$ or 4 and $n_2 = 1$ or 3. Let $P \in \mathrm{Syl}_3(G)$ and $Q \in \mathrm{Syl}_2(G)$. We distinguish cases:

- If $n_3 = 1$, then $P \triangleleft G$ and $G = P \rtimes Q$. It is enough to find all homomorphisms $\varphi\colon Q \to \mathrm{Aut}(\mathbb{Z}_3) = \mathbb{Z}_2$. We distinguish cases:

  (a) If $Q = \mathbb{Z}_4 = \langle [a] \rangle$ and $\mathbb{Z}_2 = \langle [1] \rangle$, then we have two possible homomorphisms $[a] \mapsto 0$ (the trivial one) and $[a] \mapsto [1]$ (nontrivial), which give us two non-isomorphic semidirect products $G = \mathbb{Z}_3 \times \mathbb{Z}_4 = \mathbb{Z}_{12}$ (abelian) and $G = \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ (non-abelian). If we change the choice of the generator $[a]$, then by Exercise 5.8 we get isomorphic semidirect products.

  (b) If $Q = \mathbb{Z}_2 \times \mathbb{Z}_2 = \langle [a] \rangle \times \langle [b] \rangle$ and $\mathbb{Z}_2 = \langle [1] \rangle$, then there are 4 possible homomorphisms:

  $$\begin{aligned} \varphi_1 &\colon [a] \mapsto [0], \quad [b] \mapsto [0], \\ \varphi_2 &\colon [a] \mapsto [1], \quad [b] \mapsto [0], \\ \varphi_3 &\colon [a] \mapsto [0], \quad [b] \mapsto [1], \\ \varphi_4 &\colon [a] \mapsto [1], \quad [b] \mapsto [1]. \end{aligned}$$

  The homomorphism φ_1 gives us the abelian group $G = P \rtimes_{\varphi_1} Q = \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Now, $\varphi_2, \varphi_3, \varphi_4$, by Exercise 5.8, give isomorphic non-abelian semidirect products $G = \mathbb{Z}_3 \rtimes_{\varphi_2} (\mathbb{Z}_2 \times \mathbb{Z}_2)$.

  The semidirect products in (a) and (b) are pairwise non-isomorphic (why?).

- If $n_3 = 4$, then $n_2 = 1$, therefore $Q \triangleleft G$ and $G = Q \rtimes_\varphi P$. We distinguish cases:

  (a) If $Q = \mathbb{Z}_4$, then the unique homomorphism $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$ is the trivial one, and $G = \mathbb{Z}_{12}$.

  (b) If $Q = \mathbb{Z}_2 \times \mathbb{Z}_2$, then $\mathrm{Aut}(Q) \cong \mathrm{GL}_2(\mathbb{Z}_2)$. If $\varphi\colon \mathbb{Z}_3 \to \mathrm{GL}_2(\mathbb{Z}_2)$, then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. If φ is nontrivial, then φ is one-to-one and its image is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ of order 3, of which there is a unique such subgroup. Hence, by Exercise 5.9, there is a unique such semidirect product induced by a nontrivial homomorphism $\varphi\colon \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$.

  The semidirect products in (a) and (b) are pairwise non-isomorphic (why?).

The semidirect products in the above cases are pairwise non-isomorphic. Hence, in total there are exactly 5 groups of order 12, up to isomorphism, of which 3 are non-abelian.

■

Chapter 6

Free Abelian Groups

Problem 6.1. Show that every finitely generated abelian group is an epimorphic image of a free abelian group.

Solution. Let $G = \langle g_1, \ldots, g_n \rangle$ be abelian, and let $F = \bigoplus_{i=1}^{n} \mathbb{Z}_i$, where $\mathbb{Z}_i = \langle x_i \rangle$ is infinite cyclic. Consider the map $x_i \mapsto g_i$. By the universal property of free abelian groups, the previous map extends to an epimorphism $F \to G$. ■

Problem 6.2. Let $\pi \colon G \to H$ be an epimorphism of abelian groups. If there exists a homomorphism $\varphi \colon F \to H$, where F is free abelian, then there exists $\psi \colon F \to G$ such that the following diagram is commutative.

$$\begin{tikzcd} G \arrow[r, "\pi"] & H \\ F \arrow[u, "\psi"] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Solution. Let $\{x_i\}$ be a basis of F. Since each $\varphi(x_i) \in H$ and π is onto, there exists $g_i \in G$ such that $\pi(g_i) = \varphi(x_i)$. The map $x_i \mapsto g_i$, by the universal property of free abelian groups, extends to $\psi \colon F \to G$ with $\pi \circ \psi = \varphi$. ■

Problem 6.3. Let G be an abelian group, let F be a free abelian group, and let $\pi \colon G \to F$ be an epimorphism of groups. Then $G = \ker \pi \oplus H$, where $H \cong F$.

Solution. From the previous exercise, through $F \xrightarrow{\text{id}} F$ and $G \xrightarrow{\pi} F$, there exists a homomorphism $\varphi \colon F \to G$ such that $\pi \circ \varphi = \text{id}$. Hence, φ is one-to-one and $F \cong \text{Im}\varphi$. Define $H = \text{Im}\varphi$. We will show that $G = \ker \pi \oplus H$.

- We have $\ker\pi, H \lhd G$, since G is abelian.
- Let $g \in \ker\pi \cap H$. That is, $g = \varphi(x)$, for some $x \in F$, and $g \in \ker\pi$. Thus $x = \pi\circ\varphi(x) = 1$.
- We will show that $G = \ker\pi \cdot H$. Let $g \in G$. Then we have $\pi \circ \varphi \circ \pi(g) = \pi(g)$, that is, $g^{-1}\varphi(\pi(g)) \in \ker\pi$, hence $g \in \ker\pi \cdot H$.

■

Problem 6.4. Let F be a free abelian group of rank n, and let $0 \lneqq H \leq F$. Then H is free abelian with $\mathrm{rank}(H) \leq n$.

Solution. We will prove the desired result by induction on n.

- Let $n = 1$. Then $F \cong \mathbb{Z}$, infinite cyclic. If H is a nontrivial subgroup of F, then it is also infinite cyclic, and we have the desired result.
- Suppose that the desired result holds for every $1 \leq m < n$. Let H be a nontrivial subgroup of F. We have $F = \bigoplus_{i=1}^{n} \mathbb{Z}_i$, with each $\mathbb{Z}_i$ infinite cyclic. Let $K = \bigoplus_{i=1}^{n-1} \mathbb{Z}_i$. We distinguish cases:
    1. If $H \leq K$, since K is free of rank $n-1$, by the induction hypothesis H is free with $\mathrm{rank}(H) \leq \mathrm{rank}(K) = n-1 < n$.
    2. If $H \nleq K$, then consider the natural epimorphism $\pi\colon F \to \mathbb{Z}$ with $\ker\pi = K$. Since $H \nleq K$, we have $\pi(H) \neq 0$, hence $\pi(H) = \mathbb{Z}$. Therefore, the restriction $\pi\colon H \to \mathbb{Z}$ is an epimorphism. From the previous exercise, we have $H = \ker\pi\big|_H \oplus \mathbb{Z}$. But $\ker\pi\big|_H = K \cap H \leq K$. By the induction hypothesis, $\ker\pi\big|_H$ is free of rank $m \leq n-1$. Therefore,
    $$H = \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{m} \oplus \mathbb{Z},$$
    hence H is free abelian with $\mathrm{rank}(H) = m + 1 \leq n$.

■

Problem 6.5. If an abelian group G is generated by n elements, then every subgroup of it can be generated by at most n elements.

Solution. Consider an epimorphism $\pi\colon F \to G$, that is, $G \cong F/K$, where $K = \ker\pi$. Then, by the correspondence theorem, there exists $\Lambda \leq F$ with $K \leq \Lambda$ such that $H \cong \Lambda/K$. But F is free of rank n, therefore Λ is free of rank $m \leq n$, that is, $\Lambda/K = \langle g_1, \ldots, g_m \rangle$. Hence, H is generated by m elements. ■

Problem 6.6. Let $F = \mathbb{Z}^n$. Show that F cannot be generated by fewer than n elements.

Solution. Suppose that F is generated by m elements. Therefore, there exists an epimorphism $\pi\colon \mathbb{Z}^m \to \mathbb{Z}^n$. Hence, by Exercise 6.3, we have $\mathbb{Z}^m = \ker \pi \oplus \mathbb{Z}^n$. Thus

$$m = \operatorname{rank}(\mathbb{Z}^m) \geq \operatorname{rank}(\ker \pi) + \operatorname{rank}(\mathbb{Z}^n) \geq n.$$

■

Problem 6.7. Let F be a free abelian group of finite rank and let $H \leq F$. Show that $|F/H|$ is finite if and only if $\operatorname{rank}(F) = \operatorname{rank}(H)$.

Solution. First, suppose that $|F/H| = k$. If $x_1, \ldots, x_n$ is a basis of F, then $kx_i \in H$, for every i. Define a map $x_i \mapsto kx_i$, which extends to a monomorphism $F \to H$. Hence, $\operatorname{rank}(F) \leq \operatorname{rank}(H)$.

Conversely, suppose that $\operatorname{rank}(F) = \operatorname{rank}(H)$. Since F/H is a finitely generated abelian group, by the structure theorem for abelian groups, it is enough to show that every element of it has finite order. If $F = \bigoplus_{i=1}^n \mathbb{Z}_i$ with $\mathbb{Z}_i = \langle x_i \rangle$ infinite cyclic, it is enough to show that x_iH has finite order, for every i.

Suppose, for contradiction, that there exists x_i such that $H \cap \langle x_i \rangle = \emptyset$. Then the restriction of the canonical projection to H, $\pi\colon H \to F/\langle x_i \rangle$, is a monomorphism, that is, $H \hookrightarrow F/\langle x_i \rangle$, where $F/\langle x_i \rangle$ is free of rank $n-1$, a contradiction. Therefore, for every i, there exists k_i such that $k_i x_i \in H$. ■

Problem 6.8. If G is a free abelian group of finite rank and $\varphi\colon G \to H$ is an epimorphism, then $\operatorname{rank}(G) = \operatorname{rank}(\ker \varphi) + \operatorname{rank}(H)$.

Solution. First, H is isomorphic to a quotient of G, hence it is a finitely generated abelian group. By the structure theorem for abelian groups, there exists k such that kH is free abelian of rank $\operatorname{rank}(H)$. Consider the epimorphism $\psi\colon H \to kH$ given by $h \mapsto kh$. Therefore, applying Exercise 6.3 to $\psi \circ \varphi$, we obtain

$$\operatorname{rank}(G) = \operatorname{rank}(\ker(\psi \circ \varphi)) + \operatorname{rank}(H).$$

Hence, it is enough to show that $\operatorname{rank}(\ker(\psi \circ \varphi)) = \operatorname{rank}(\ker \varphi)$. Initially, it is clear that $\ker \varphi \leq \ker(\psi \circ \varphi)$. Hence, by Exercise 6.7, it is enough to show that $\ker(\psi \circ \varphi)/\ker \varphi$ is a finite group. Since it is a finitely generated abelian group (why?), it is enough to show that every element has finite order. Indeed, if $x \in \ker(\psi \circ \varphi)$, then we have $\varphi(kx) = 0$, that is, $kx \in \ker \varphi$, and we have the desired result. ■

Problem 6.9. Let F be a free abelian group of rank n. Prove that $\operatorname{Aut}(F) \cong \operatorname{GL}_n(\mathbb{Z})$.

Chapter 7

Solvable Groups

Problem 7.1. Show that $\mathfrak{S}_3, \mathfrak{S}_4$ are solvable.

Solution. Immediate, since $|\mathfrak{S}_3| = 2 \cdot 3$ and $|\mathfrak{S}_4| = 2^3 \cdot 3$. ∎

Problem 7.2. If G is a group with $|G| < 100$ and $|G| \neq 60$, then G is solvable.

Problem 7.3. Examine whether a group G with $|G| = 144$ is solvable.

Solution. We have $|G| = 2^4 \cdot 3^2$. Also, $n_3 = 1$ or 4 or 16. We distinguish cases.

(a) If $n_3 = 1$, then there exists a normal $P \in \mathrm{Syl}_3(G)$, which is solvable as a p-group, and G/P is solvable as a p-group. Therefore, G is solvable.

(b) If $n_3 = 4$, then $[G : \mathrm{N}_G(P)] = 4$. Through the action of G on the cosets G/P, a homomorphism $\varphi\colon G \to \mathfrak{S}_4$ is induced, with $\ker\varphi \leq \mathrm{N}_G(P)$ solvable as a subgroup of a solvable group, and $G/\ker\varphi \cong \mathrm{Im}\varphi \leq \mathfrak{S}_4$ solvable as a subgroup of $\mathfrak{S}_4$, which is solvable.

(c) If $n_3 = 16$, we distinguish cases:

- If any two Sylow 3-subgroups have trivial intersection, then there are $16(9-1) = 128$ elements of order a power of 3. Therefore, there exists a unique Sylow 2-subgroup of G, say Q, which is solvable as a p-group. Also, G/Q is solvable as a p-group, hence G is solvable.
- Suppose that there exist $P, Q \in \mathrm{Syl}_2(G)$ with $P \neq Q$ and $P \cap Q \neq 1$. Then $P, Q \subsetneqq \mathrm{N}_G(P \cap Q)$, hence $|N_G(P \cap Q)| = 2 \cdot 3^2,\ 2^2 \cdot 3^2,\ 2^3 \cdot 3^2,\ 2^4 \cdot 3^2$. If $|\mathrm{N}_G(P \cap Q)| = 2 \cdot 3^2,\ 2^2 \cdot 3^2,\ 2^3 \cdot 3^2$, the desired result follows similarly to (b). If $|\mathrm{N}_G(P \cap Q)| = 2^4 \cdot 3^2$, then $\mathrm{N}_P(P \cap Q) = G$, therefore $P \cap Q$ is solvable and normal in G, with $G/(P \cap Q)$ normal in G, hence G is solvable.

■

Problem 7.4. If $M, N \leq G$ and M, N are solvable with $M \triangleleft G$, then MN is solvable.

Solution. Use that $MN/N \cong M/M \cap N$. ■

Problem 7.5. If $M, N \triangleleft G$ and $G/M, G/N$ are solvable, then $G/M \cap N$ is solvable.

Solution. Consider the homomorphism $\varphi\colon G \to G/M \times G/N$ given by $\varphi(g) = (gM, gN)$. ■

Problem 7.6. If $K \leq L \leq M$, where K is fully invariant in L and L is fully invariant in M, show that K is fully invariant in M.

Solution. Let $\varphi \in \operatorname{End}(M)$. Then $\varphi|_L \in \operatorname{End}(L)$, since L is a fully invariant subgroup of M. Hence, we have $\varphi(K) = \varphi|_L(K) \subseteq K$, since K is a fully invariant subgroup of L. ■

Problem 7.7. Let G be a group, and let $G^{(n)}$ be the terms of the derived series. Prove that $G^{(n)}$ is a fully invariant subgroup of G, for every $n \in \mathbb{N}$.

Solution. Immediate by induction. ■

Problem 7.8. A finite solvable group contains a fully invariant abelian p-subgroup for some prime p.

Problem 7.9. Let G be a finite solvable group. If $N \neq 1$ is a minimal normal subgroup of G, show that $N = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, where p is prime.

Solution. First, N is solvable as a subgroup of a solvable group. We have that N' is a characteristic subgroup of N, and since N is normal in G, it follows that N' is normal in G. Consequently, either $N = N'$ or $N' = 1$. If $N = N'$, then the derived series would be constant, and we arrive at a contradiction from the solvability of N. Therefore, $N' = 1$, that is, N is finite abelian. Hence, N is the product of its Sylow subgroups. If P is a Sylow p-subgroup of N, since it is characteristic in N, we similarly have $N = P$. If we show that every nontrivial element of N has order p, we have the desired result. Let

$$A = \{g \in N \mid g^p = 1\}.$$

The subgroup A is characteristic in N, and therefore similarly we have $N = A$. ■

Chapter 8

Nilpotent Groups

Problem 8.1. Let G be a nilpotent group. If N is a nontrivial normal subgroup of G, then $N \cap \mathrm{C}(G) \neq \{1\}$. If, moreover, N is a minimal normal subgroup, then $N \subseteq \mathrm{C}(G)$.

Solution. The group G is nilpotent, and let its central series be $1 \subseteq \mathrm{C}(G) \subseteq \mathrm{C}^2(G) \subseteq \cdots \subseteq \mathrm{C}^n(G) = G$. Let k be the smallest positive integer such that $N \cap \mathrm{C}^k(G) \neq 1$. Then, since the above series is central and N is normal, we have

$$\left[\mathrm{C}^k(G), G\right] \subseteq \mathrm{C}^{k-1}(G) \Rightarrow \left[\mathrm{C}^k(G) \cap N, G\right] \subseteq \mathrm{C}^{k-1}(G) \cap N = \{1\}.$$

Hence, $\mathrm{C}^k(G) \cap N \subseteq \mathrm{C}(G)$, that is, $1 \neq \mathrm{C}^k(G) \cap N \subseteq \mathrm{C}(G) \cap N$. ■

Problem 8.2. Let G be a group and let $N \leq \mathrm{C}(G)$. Show that G is nilpotent if and only if G/N is nilpotent.

Solution. From Exercise 3.4, every Sylow p-subgroup of G/N is of the form PN/N, where $P \in \mathrm{Syl}_p(G)$. Hence, G has a unique normal Sylow p-subgroup if and only if G/N has a unique normal Sylow p-subgroup. ■

Problem 8.3. If the automorphism group $\mathrm{Aut}(G)$ of a group G is nilpotent, then G is also nilpotent.

Solution. Observe that $G/\mathrm{C}(G) \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ through the homomorphism $g \mapsto \tau_g$. Therefore, $G/\mathrm{C}(G)$ is nilpotent, that is, it has a central series, by the correspondence theorem,

$$1 = \mathrm{C}(G)/\mathrm{C}(G) \lhd \mathrm{C}^2/\mathrm{C}(G) \lhd \mathrm{C}^3/\mathrm{C}(G) \lhd \cdots \lhd \mathrm{C}^n/\mathrm{C}(G) = G/\mathrm{C}(G),$$

with $\mathrm{C}(G) \subseteq \mathrm{C}^i$, for every i. Observe that

$$1 \lhd \mathrm{C}(G) \lhd \mathrm{C}^2 \lhd \mathrm{C}^3 \lhd \cdots \lhd \mathrm{C}^n = G.$$

■

Problem 8.4. Let G be a finite nilpotent group and let $H \leq G$ with $[G : H] = n$. Prove that $g^n \in H$, for every $g \in G$.

Solution. Since $H \leq G$, it is subnormal, that is, there exists a normal series $H_0 = H \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n$. We have

$$n = [G : H] = [G : H_{n-1}] \cdot [H_{n-1} : H_{n-2}] \cdots [H_2 : H_1] \cdot [H_1 : H].$$

If $[H_i : H_{i-1}] = n_i$ and $g \in G$, then $g^{n_1} \in H_{n-1}$. Thus $g^{n_1 n_2} \in H_{n-2}$. Continuing in finitely many steps, we obtain $g^n \in H$. ■

Problem 8.5. Let G be a finite group. Prove that:

(a) G is nilpotent if and only if, for every pair of elements $a, b \in G$ with $(o(a), o(b)) = 1$, we have $ab = ba$.

(b) G is nilpotent if and only if, for every divisor n of the order of G, there exists a normal subgroup of order n.

Solution. (a) Since G is nilpotent, we have $G = P_1 \times \cdots \times P_n$, the direct product of its Sylow subgroups. Let $a, b \in G$ with $(o(a), o(b)) = 1$. Then $a = \prod_i^n a_i$ and $b = \prod_{i=1}^n b_i$. Since $(o(a), o(b)) = 1$, we have $I = \{i \in \{1, \ldots, n\} \mid a_i, b_i \neq 1\} = \emptyset$, therefore it is clear that $ab = ba$.

Conversely, suppose that for every pair of elements $a, b \in G$ with $(o(a), o(b)) = 1$, we have $ab = ba$. Then $G = P_1 \cdots P_n$, where $P_i \in \mathrm{Syl}_{p_i}(G)$ and $|G| = p_1^{a_1} \cdots p_n^{a_n}$. It is enough to show that every P_i is normal. Let $i \in \{1, \ldots, n\}$. For every j, we have $P_j \subseteq \mathrm{N}_G(P_i)$. Therefore, $G = \mathrm{N}_G(P_i)$, which is the desired result.

(b) Suppose that G is nilpotent with $|G| = n = p_1^{a_1} \cdots p_n^{a_n}$. Let $\nu | n$, that is, $\nu = p_1^{b_1} \cdots p_n^{b_n}$ with $b_i \leq a_i$. If P_i is the Sylow p_i-subgroup of G, then there exists a normal subgroup N_i of P_i of order $p_i^{b_i}$. Then $N = N_1 \times \cdots \times N_n$ is a normal subgroup of G of order ν. The converse is immediate, since every Sylow subgroup of G is normal.

■

Problem 8.6. Let G be a nilpotent group of class $c > 1$. For every $a \in G$, the subgroup $H = \langle a, G' \rangle$ is nilpotent of class less than c.

Solution. Since G is nilpotent of class c, we have $\mathrm{C}^c(G) = G$ and $\mathrm{C}^{c-1}(G) \neq G$. Since $G/\,\mathrm{C}^{c-1}(G) = \mathrm{C}^c(G)/\,\mathrm{C}^{c-1}(G)$ is abelian, we have $G' \subseteq \mathrm{C}^{c-1}(G)$, hence $G' \subseteq \mathrm{C}^{c-1}(G) \cap H = \mathrm{C}^{c-1}(H)$. Thus $H/\,\mathrm{C}^{c-1}(H) = \langle \overline{a} \rangle$ is cyclic. We observe that

$$H/\,\mathrm{C}^{c-1}(H) \cong \big(H/\,\mathrm{C}^{c-2}(H)\big) \,/\, \big(\mathrm{C}^{c-1}(H)/\,\mathrm{C}^{c-2}(H)\big) = \Gamma/Z(\Gamma),$$

where $\Gamma = H/\,\mathrm{C}^{c-2}(H)$. Since the above quotient is cyclic, Γ is abelian and $\Gamma = Z(\Gamma)$. Therefore, $H = \mathrm{C}^{c-1}(H)$, that is, the nilpotency class of H is less than c. ■

Problem 8.7. In a nilpotent torsion-free group G, extraction of roots is unique. That is, if $a^n = b^n$, for $n > 0$, then $a = b$.

Solution. We prove the desired result by induction on the nilpotency class of G.

- If $c = 1$, then G is abelian, and we observe that if $a^n = b^n$, then $(a^{-1}b)^n = 1$. Since G is torsion-free, we have $a = b$.

- If $c > 1$, then by Exercise 8.6, the nilpotency class of $H = \langle a, G' \rangle$ is less than c. Since $a, b^{-1}ab \in H$, by the induction hypothesis we have
$$\left(b^{-1}ab\right)^n = b^{-1}a^n b = b^n = a^n.$$
Therefore, $ab = ba$. Similarly as before, it follows that $a = b$.

■

Problem 8.8. Suppose that G is a finite group all of whose maximal subgroups are simple and normal. Show that G is abelian and $|G| = 1, p, p^2, pq$, where p, q are primes.

Solution. Since every maximal subgroup of G is normal, G is nilpotent. Therefore, by Exercise 8.5, the possible orders of G are $1, p, p^2, pq$. We know that every group of order $1, p, p^2$ is abelian. Now, if $|G| = pq$ and G is nilpotent, then as the direct product of its Sylow subgroups, G is cyclic, hence abelian. ■

Problem 8.9. Show that every group of order 90 is not simple and is solvable. Is it necessarily nilpotent?

Solution. Let G be a group with $|G| = 90 = 2 \cdot 3^2 \cdot 5$. We have $n_5 = 1$ or 6. If $n_5 = 1$, then G has a unique normal Sylow 5-subgroup, and we have the desired result. If $n_5 = 6$, then $n_3 = 1$ or 10. If $n_3 = 1$, we are done. If $n_3 = 10$, we distinguish cases:

- If any two Sylow 3-subgroups intersect trivially, then there are $10(3^2 - 1) = 80$ elements of order a power of 3, and we arrive at a contradiction, since there are $6(5-1) = 24$ elements of order a power of 5.

- If there exist distinct $P, Q \in \mathrm{Syl}_3(G)$ with $P \cap Q \neq 1$, then it follows that $P, Q \subsetneqq N_G(P \cap Q) = N$, therefore N has order $3^2 \cdot 5$ or $3^2 \cdot 2$, or $N = G$. In each of the following cases, it is proved that G is not simple.

Now, if N is a nontrivial proper subgroup of G, then N and G/N are solvable (check their orders), therefore G is solvable.

A group G of order 90 is not necessarily nilpotent. Consider the nontrivial homomorphism $\varphi \colon \mathbb{Z}_{18} \to \mathrm{Aut}(\mathbb{Z}_5) = \mathbb{Z}_4$ with $[1]_{18} \mapsto [1]_4$, and let $G = \mathbb{Z}_5 \rtimes_\varphi \mathbb{Z}_{18}$. If G were nilpotent, then it would be the direct product of its Sylow subgroups, that is, the direct product of $\mathbb{Z}_5$ and $\mathbb{Z}_{18}$, which cannot hold since φ is nontrivial. ■

Chapter 9

Free Groups and Free Products

Problem 9.1. Show that every free product $*_{a \in J} G_a$ with $|J| \geq 2$ and $G_a \neq \{1\}$, for every $a \in J$, has an element of infinite order.

Solution. Let $a_1 \neq a_2 \in J$ and let $g_i \in G_{a_i}$ be nontrivial. Then $g^n = \underbrace{(g_1 g_2) \cdots (g_1 g_2)}_{n \text{ times}}$ is in reduced form, hence $g^n \neq 1$, for every $n \geq 1$. ■

Problem 9.2. Let $\{G_a\}_{a \in J}$ be a family of groups with $|J| \geq 2$. If $G = *_a G_a$, show that $Z(G) = \{1\}$.

Solution. Let $1 \neq g = g_1 \cdots g_n \in G$ be in reduced form. Since $|J| \geq 2$, there exists $g_{n+1} \notin G_{a_n}$. The word $g g_{n+1} = g_1 \cdots g_n g_{n+1}$ is in reduced form of length $n+1$. If $g_{n+1} \in G_{a_1}$, then the reduced form of $g_{n+1} g$ has length n, that is, it is different from $g g_{n+1}$, while if $g_{n+1} \notin G_{a_1}$, then the word $g_{n+1} g$ is in reduced form. If $g_{n+1} g = g g_{n+1}$, then by the uniqueness of reduced forms $g_n = g_{n+1}$, hence we arrive at a contradiction. ■

Problem 9.3. If $G = G_1 * G_2$ and N_1 is the normal subgroup of G generated by the factor G_1, show that $N_1 \cap G_2 = \{1\}$.

Solution. We know that

$$N_1 = \left\{ \prod_{i=1}^{n} x_i g_i x_i^{-1} \mid n \in \mathbb{N},\ x_i \in G,\ g_i \in G_1 \right\}.$$

Observe that there is no nontrivial element in the intersection $N_1 \cap G_2$, since every word $\prod_{i=1}^{n} x_i g_i x_i^{-1}$ in its reduced form contains an element of G_1. ■

Problem 9.4. Every element of finite order in a free product $*_{a\in J}G_a$ is contained in a conjugate of a free factor.

Solution. We will prove the desired result by induction on the length of the word. Let $g = g_1 \cdots g_n \in *G_a$ be of finite order and in reduced form. Then $g_1, g_n \in G_{a_1}$. We have that $g_1^{-1}gg_1$ is a reduced word of length $n-1$, hence by the induction hypothesis there exist $w \in G$ and $g_k \in G_{a_k}$, for some $k \in J$, such that $g_1^{-1}gg_1 = w^{-1}g_kw$, that is, $g = (wg_1^{-1})^{-1}g_k(wg_1^{-1})$, and we have the desired result. ■

Problem 9.5. Every finite subgroup of a free product is contained in a conjugate of a free factor.

Solution. We will prove a more general result. If in a subgroup of a free product every element has finite order, then it is contained in a conjugate of a free factor. Let $G = *_aG_a$ and let H be a nontrivial subgroup of G, where every element of it has finite order. Let $x \in H$, so as an element of finite order we have $x = gg_ag^{-1}$, where $g \in G$ and $g_a \in G_a$. If $y = hg_bh^{-1}$, where $h \in G$ and $g_b \in G_b$, it is enough to show that $g = h$ and $a = b$. Since $xy \in H$, it must have finite order. Using this, show the desired result. ■

Problem 9.6. If $G = *_{a\in J}G_a$ and each G_a decomposes as a free product $G_a = *_bH_{ab}$, then G is the free product of all the H_{ab}. This is called a refinement of the original one.

Solution. Immediate by using the universal property of free products. ■

Problem 9.7. If $G = *_{a\in J}G_a$ and for every $a \in J$ we have a subgroup $H_a \leq G_a$, then the group generated by the H_a is isomorphic to their free product. That is, $\langle H_a \mid a \in J\rangle = *_{a\in J}H_a$.

Solution. Immediate, since for every $h = h_1 \cdots h_n$ in reduced form with $h_j \in H_{a_j}$, for every j with $n \geq 2$, we have $h \neq 1$. ■

Problem 9.8. If $G = *_{a\in J}G_a$ and G' is the derived subgroup of G, then $G/G' \cong \bigoplus_{a\in J} G_a/G'_a$.

Solution. We will show that G/G' satisfies the universal property of direct sums. For every a, consider the homomorphism

$$\begin{tikzcd} G_a \arrow[r, "i_a"] \arrow[rr, bend right, "\mu_a"'] & G \arrow[r, "\pi"] & G/G' \end{tikzcd}$$

Since the quotient $G_a/\ker\mu_a$ is abelian, we have $G'_a \subseteq \ker\mu_a$, and by the universal property of quotient groups there is a unique homomorphism $G_a/G'_a \xrightarrow{\varphi_a} G/G'$ which makes the following diagram commutative:

$$\begin{tikzcd} G_a \arrow[r, "\mu_a"] \arrow[d, "\pi_a"'] & G/G' \\ G_a/G'_a \arrow[ur, "\varphi_a"'] & \end{tikzcd}$$

We will prove that the triplet $(G/G', G_a/G'_a, \varphi_a)$ satisfies the universal property of direct sums. Let H be an abelian group and let $G_a/G'_a \xrightarrow{\psi_a} H$ be homomorphisms. Then homomorphisms $G_a \xrightarrow{\nu_a=\psi_a\circ\pi_a} H$ are induced, where by the universal property of free products there exists a unique homomorphism $G \xrightarrow{\nu} H$ which, for every a, makes the following diagram commutative:

$$\begin{tikzcd} G_a \arrow[r, "\nu_a=\psi_a\circ\pi_a"] \arrow[d, "i_a"'] & H \\ G \arrow[ur, "\nu"'] & \end{tikzcd}$$

Since the quotient $G/\ker\nu$ is an abelian group, we have $G' \subseteq \ker\nu$, and by the universal property of quotient groups there exists a homomorphism $G/G' \xrightarrow{\varphi} H$ such that the following diagram is commutative:

$$\begin{tikzcd} G \arrow[r, "\nu"] \arrow[d, "\pi"'] & H \\ G/G' \arrow[ur, "\varphi"'] & \end{tikzcd}$$

First, we must show that for every a the following diagram is commutative:

$$\begin{tikzcd} G_a/G'_a \arrow[r, "\psi_a"] \arrow[d, "\varphi_a"'] & H \\ G/G' \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Let $g_aG'_a \in G_a/G'_a$. Then

$$\begin{aligned} & \varphi\circ\varphi_a(g_aG'_a) = \varphi\circ\varphi_a\circ\pi_a(g_a) = \varphi\circ\mu_a(g_a) \\ = \quad & \varphi\circ\pi\circ i_a(g_a) = \nu\circ i_a(g_a) = \psi_a\circ\pi_a(g_a) = \psi_a(g_aG'_a). \end{aligned}$$

For the uniqueness of φ, suppose that $\psi\colon G/G' \to H$ is such that for every a the following diagram is commutative:

$$\begin{tikzcd} G_a/G'_a \arrow[r, "\psi_a"] \arrow[d, "\varphi_a"'] & H \\ G/G' \arrow[ur, "\psi"'] & \end{tikzcd}$$

It is enough to show equality on the generators $g_aG' \in G/G'$. Indeed,

$$\begin{aligned} & \varphi(g_aG') = \varphi \circ \pi \circ i_a(g_a) = \varphi \circ \varphi_a \circ \pi_a(g_a) \\ = \; & \psi_a(g_aG'_a) = \psi \circ \varphi_a \circ \pi_a(g_a) \\ = \; & \psi \circ \pi \circ i_a(g_a) = \psi(g_aG'). \end{aligned}$$

■

Problem 9.9. Let $G = *_{a\in J}G_a$, where each factor is nontrivial. If G is finitely generated, then:

(a) The index set I is finite.

(b) Every factor G_i is a finitely generated group.

Solution. ■

Problem 9.10. Let $G_i,\ i \in I$, be a family of groups with presentations $G_i = \langle X_i \mid R_i\rangle$. Show that

$$*_{i\in I}G_i = \left\langle \bigsqcup_{i\in I} X_i \mid \bigsqcup_{i\in I} R_i \right\rangle.$$

Solution. Let $G = \langle \bigsqcup_{i\in I} X_i \mid \bigsqcup_{i\in I} R_i\rangle$. Consider the homomorphisms

$$\begin{tikzcd} F(X_j) \arrow[r, "i_j"] \arrow[rr, bend right, "\mu_j"'] & F\left(\bigsqcup_{i\in I} X_i\right) \arrow[r, "\pi"] & G \end{tikzcd}$$

where i_j is the homomorphism on free groups induced by $x_j \mapsto (j, x_j)$. If $N_j = \langle\langle R_j\rangle\rangle$, then since $N_j \subseteq \ker \mu_j$, homomorphisms $\varphi_j\colon G_j \to G$ are induced which make the following diagram commutative:

$$\begin{tikzcd} F(X_j) \arrow[r, "\mu_j"] \arrow[d, "\pi_j"'] & G \\ G_j \arrow[ur, "\varphi_j"'] & \end{tikzcd}$$

We will show that the triplet (G, G_j, φ_j) satisfies the universal property of free products. Let H be a group and let $G_j \xrightarrow{\psi_j} H$ be homomorphisms. Through the maps $X_j \xrightarrow{a_j} G_j$, maps are induced

$$\begin{tikzcd} X_j \arrow[r, "a_j"] \arrow[rr, bend right, "b_j"'] & G_j \arrow[r, "\psi_j"] & H \end{tikzcd}$$

from which a map $\bigsqcup_{i \in I} X_i \xrightarrow{c} H$ is induced, making the following diagram commutative:

$$\begin{tikzcd} X_j \arrow[r, "b_j"] \arrow[d, "i'_j"'] & H \\ \bigsqcup_{i \in I} X_i \arrow[ur, "c"'] & \end{tikzcd}$$

By the universal property of free groups, a homomorphism $\hat{\varphi} \colon F\left(\bigsqcup_{i \in I} X_i\right) \to H$ is induced. Then, by the universal property of quotient groups (why?), a homomorphism $G \xrightarrow{\varphi} H$ is induced, making the following diagram commutative:

$$\begin{tikzcd} F\left(\bigsqcup_{i \in I} X_i\right) \arrow[r, "\hat{\varphi}"] \arrow[d, "\pi"'] & H \\ G \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Show that φ, for every $j \in I$, makes the following diagram commutative:

$$\begin{tikzcd} G_j \arrow[r, "\psi_j"] \arrow[d, "\varphi_j"'] & H \\ G \arrow[ur, "\varphi"'] & \end{tikzcd}$$

and show that it is the unique one with this property. ■

Problem 9.11. Let G be a group and let N be a normal subgroup of G. If G/N is free, then there exists a subgroup H of G with $G = HN$ and $H \cap N = 1$.

Solution. The group G/N is free, hence $G/N = *_{a \in J} G_a$. By the correspondence theorem, for every $a \in J$ there exists $\tilde{G}_a$ in G with $N \subseteq \tilde{G}_a$ such that $\tilde{G}_a/N = G_a$. Let $\hat{G}_a = \tilde{G}_a \setminus N$ and $H = \left\langle \hat{G}_a \mid a \in J \right\rangle$. Show that H satisfies the desired properties. ■

Problem 9.12. Let F be free and let H be a subgroup of F of finite index. If K is a nontrivial subgroup of F, then $K \cap H \neq 1$.

Solution. Let $1 \neq x \in K$. Let N be the normal subgroup arising from the action of G on the cosets G/H. Then we know that $[G : N] = n < \infty$. We distinguish cases:

- If $x \in H$, we have the desired result.
- If $x \notin H$ and its reduced form has length greater than 2, then $o(x) = \infty$, hence $x^n \neq 1$ and $x^n \in K \cap N \subseteq K \cap H$.
- If $x \notin H$ and it has length 1 in its reduced form, then x belongs to one of the factors of F, hence $o(x^n) = \infty$, and similarly to the above we have the desired result.

■

Chapter 10

Free Products with Amalgamation

Problem 10.1 (Universal property of the free product with amalgamation)**.** Let $G_\lambda,\ \lambda \in \Lambda$, be a family of groups, let H be a group, let $\varphi_\lambda\colon H \to G_\lambda$ be a family of monomorphisms, and let $G = *_H G_\lambda$ be the corresponding free product with amalgamation. Prove that for every group K and every family of homomorphisms $\vartheta_\lambda\colon G_\lambda \to K$ with $\vartheta_\lambda \circ \varphi_\lambda = \vartheta_\mu \circ \varphi_\mu$ for every pair $\lambda, \mu \in \Lambda$, there exists a unique homomorphism $\vartheta\colon G \to K$ such that $\vartheta \circ \pi_\lambda = \vartheta_\lambda$ for every λ, where π_λ is the restriction to G_λ of the natural epimorphism $\pi\colon *_\lambda G_\lambda \to G$.

Solution. By the universal property of free products, there exists a unique homomorphism $\varphi\colon *_\lambda G_\lambda \to K$ such that, for every λ, the following diagram is commutative:

$$\begin{tikzcd}
*_\lambda G_\lambda \arrow[r, "\varphi"] & K \\
G_\lambda \arrow[u, "i_\lambda"] \arrow[ur, "\vartheta_\lambda"'] &
\end{tikzcd}$$

If $R = \left\{\varphi_\lambda(h)\,(\varphi_\mu(h))^{-1} \mid h \in H,\ \lambda, \mu \in \Lambda\right\}$, then $R \subseteq \ker\varphi$ (why?), hence $N = \langle\langle R \rangle\rangle \subseteq \ker\varphi$. By the universal property of quotient groups, there is a unique homomorphism $\vartheta\colon G \to K$ which makes the following diagram commutative:

$$\begin{tikzcd}
G \arrow[r, "\vartheta"] & K \\
*_\lambda G_\lambda \arrow[u, "\pi"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

Then, from the commutativity of the above diagrams, we have that for every λ the following diagram is commutative:

$$\begin{tikzcd}
G \arrow[rr, "\vartheta"] & & K \\
& *_\lambda G_\lambda \arrow[ul, "\pi"'] \arrow[ur, "\varphi"] & \\
& G_\lambda \arrow[u, "i_\lambda"] \arrow[uul, bend left, "\pi_\lambda"] \arrow[uur, bend right, "\vartheta_\lambda"'] &
\end{tikzcd}$$

where $\pi_\lambda = \pi \circ i_\lambda$. Thus $\vartheta \circ \pi_\lambda = \vartheta_\lambda$, which is the desired result. Show that ϑ is the unique homomorphism with this property by following the above diagrams. ■

Definition 10.0.1. Let $\varphi_i\colon H \to G_i$, $i = 1, 2$, be monomorphisms, let $G = G_1 *_H G_2$ be the corresponding product with amalgamation, and let $\pi\colon G_1 * G_2 \to G_1 *_H G_2$ be the natural epimorphism. A **reduced form** of an element g in G is an expression $g = \pi(g_1)\cdots\pi(g_n)$, where each $g_i \in G_1 \cup G_2$, consecutive g_i do not belong to the same factor G_1 or G_2, and for every i we have $g_i \notin \varphi_1(H) \cup \varphi_2(H)$, except possibly when $n = 1$.

Problem 10.2. (a) Every element of G can be written in reduced form.

(b) If $g = \pi(g_1)\pi(g_2)\cdots\pi(g_n)$ with $n \geq 2$, then $g \neq 1$.

(c) If $\varphi_i(H)$ is a proper subgroup of G_i, $i = 1, 2$, then the group G contains elements of infinite order.

(d) Every element of finite order of G is conjugate to an element of one of the factors G_i.

Solution.(a),(b) Immediate, since every $g \in G$ can be written uniquely in the form $g = \pi(x_0)\pi(x_1)\cdots\pi(x_n)$, where $(x_0, x_1, \ldots, x_n)$ is a $\varphi_1(H)$-normal form.

(c) Let $g_i \in G_i \setminus \varphi_i(H)$. Then the element $g = \pi(g_1)\pi(g_2)$ has infinite order by (b).

(d) Similar to Exercise 9.4.

■

Problem 10.3. Let G_1, G_2 be subgroups of a group G, and let $H = G_1 \cap G_2$. Assume that G is generated by G_1 and G_2. Let $\varphi\colon G_1 *_H G_2 \to G$ be the epimorphism induced by the inclusions of G_1 and G_2 into G. Prove that φ is an isomorphism if and only if every product $g_1 \cdots g_n$ in G, where each factor g_k belongs to $G_1 \setminus H$ or to $G_2 \setminus H$ and consecutive factors do not belong to the same set $G_i \setminus H$, is different from 1.

Solution. Through the inclusions $j_1\colon G_1 \hookrightarrow G$ and $j_2\colon G_2 \hookrightarrow G$, by the universal property of free products, an epimorphism $\psi\colon G_1 * G_2 \to G$ is induced such that the following diagram is commutative:

$$\begin{tikzcd}
G_1 \arrow[dr, "i_1"] \arrow[drr, bend left, "j_1"] & & \\
& G_1 * G_2 \arrow[r, "\psi"] & G \\
G_2 \arrow[ur, "i_2"] \arrow[urr, bend right, "j_2"'] & &
\end{tikzcd}$$

Observe that if N is the normal subgroup of the amalgam, then $N \subseteq \ker\psi$. Therefore, by the universal property of quotient groups, an epimorphism $\varphi\colon G_1 *_H G_2 \to G$ is induced such that the following diagram is commutative:

$$\begin{tikzcd}
G_1 \arrow[dr, "\pi_1"] \arrow[drr, bend left, "j_1"] & & \\
& G_1 *_H G_2 \arrow[r, "\varphi"] & G \\
G_2 \arrow[ur, "\pi_2"] \arrow[urr, bend right, "j_2"'] & &
\end{tikzcd}$$

where π_i are the restrictions of the natural epimorphism $\pi\colon G_1 * G_2 \to G_1 *_H G_2$ to G_i. Therefore, φ is an isomorphism if and only if it is one-to-one, if and only if $\varphi(g) \neq 1$ whenever $g = \pi(g_1)\cdots\pi(g_n)$ with $g \neq 1$. In particular, from the above diagrams we have $\varphi\circ\pi(g_i) = \psi(g_i) = g_i$. Therefore, $\varphi(g) = g_1\cdots g_n$. Hence, φ is an isomorphism if and only if $g_1\cdots g_n \neq 1$, where each factor g_k belongs to $G_1 \setminus H$ or to $G_2 \setminus H$, and consecutive factors do not belong to the same set $G_i \setminus H$. ■

Problem 10.4. Let $G = G_1 *_A G_2$, and let H_1, H_2 be subgroups of G_1, G_2, respectively, with $H_1 \cap A = H_2 \cap A = 1$. Show that the subgroup of G generated by the images of H_1 and H_2 is isomorphic to their free product. That is, $\langle H_1, H_2\rangle \cong H_1 * H_2$.

Solution. Let $h = \pi(h_1)\cdots\pi(h_n)$ with $n \geq 2$, where consecutive $\pi(g_i)$ belong to different factors and $\pi(g_i) \neq 1$. Since $H_1 \cap A = 1$ and $H_2 \cap A = 1$, by Exercise 10.2(b) we have $h \neq 1$, hence $\langle H_1, H_2\rangle \cong H_1 * H_2$. ■

Problem 10.5. Let $\varphi_i\colon H \to G_i,\ i = 1, 2$, be monomorphisms, let $G = G_1 *_H G_2$ be the corresponding free product with amalgamation, and let $\pi\colon G_1 * G_2 \to G_1 *_H G_2$ be the natural epimorphism. Prove that

$$\mathrm{C}(G_1 *_H G_2) = H \cap \mathrm{C}(G_1) \cap \mathrm{C}(G_2)$$

more precisely,

$$\mathrm{C}(G_1 *_H G_2) = \pi(H) \cap \mathrm{C}(\pi(G_1)) \cap \mathrm{C}(\pi(G_2)),$$

where by $\mathrm{C}(G)$ we denote the center of a group G.