Sascha Roth — Last modification: 2025-07-05
This document contains solutions of some exercises in Serge Lang's *Algebra.*

Contents

Groups

Summary

Proposition 2.1. *Let G be a group and let H, K be two subgroups such that $H \cap K = e$, $HK = G$, and such that $xy = yx$ for all $x \in H$ and $y \in K$. Then the map*

$$H \times K \to G$$

such that $(x, y) \mapsto xy$ is an isomorphism.

Proposition 2.2. *Let G be a group and H a subgroup. Then $(G : H)(H : 1) = (G : 1)$, in the sense that if two of these indices are finite, so is the third and equality holds as stated. If $(G : 1)$ is finite, the order of H divides the order of G.*

More generally, let H, K be subgroups of G and let $H \supset K$. Let $\{x_i\}$ be a set of (left) coset representatives of K in H and let $\{y_j\}$ be a set of coset representatives of H in G. Then we contend that $\{y_j x_i\}$ is a set of coset representatives of K in G.

Proposition 3.1. *Let G be a finite group. An abelian tower of G admits a cyclic refinement. Let G be a finite solvable group. Then G admits a cyclic tower whose last element is $\{e\}$.*

Theorem 3.2. *Let G be a group and H a normal subgroup. Then G is solvable if and only if H and G/H are solvable.*

Lemma 3.3. (Butterfly Lemma.) (Zassenhaus) *Let U, V be subgroups of a group. Let u, v be normal subgroups of U and V, respectively. Then*

$$\begin{gathered} u(U \cap v) \text{ is normal in } u(U \cap V), \\ (u \cap V)v \text{ is normal in } (U \cap V)v, \end{gathered}$$

and the factor groups are isomorphic, i.e.

$$u(U \cap V)/u(U \cap v) \approx (U \cap V)v/(u \cap V)v.$$

Theorem 3.4. (Shreier) *Let G be a group. Two normal towers of subgroups ending with the trivial group have equivalent refinements.*

Theorem 3.5. (Jordan-Hölder) *Let G be a group, and let*

$$G = G_1 \supset G_2 \supset \ldots \supset G_r = \{e\}$$

be a normal tower such that each group G_i/G_{i+1} is simple, and $G_i \neq G_{i+1}$ for $i = 1, ..., r-1$. Then any normal tower of G having the same properties is equivalent to this one.

Proposition 4.1. *Let G be a finite group of order $n > 1$. Let a be an element of G, $a \neq e$. Then the period of a divides n. If the order of G is a prime number p, then G is cyclic and the period of any generator is equal to p.*

Proposition 4.2. *Let G be a cyclic group. Then every subgroup of G is cyclic. If f is a homomorphism of G, then the image of f is cyclic.*

Proposition 4.3.
(i) *An infinite cyclic group has exactly two generators (if a is a generator, then a^{-1} is the only other generator).*
(ii) *Let G be a finite cyclic group of order n, and let x be a generator. The set of generators of G consists of those powers x^v of x such that v is relatively prime to n.*
(iii) *Let G be a cyclic group, and let a, b be two generators. Then there exists an automorphism of G mapping a onto b. Conversely, any automorphism of G maps a on some generator of G.*
(iv) *Let G be a cyclic group of order n. Let d be a positive integer dividing n. Then there exists a unique subgroup of G of order d.*
(v) *Let G_1, G_2 be cyclic of orders m, n respectively. If m, n are relatively prime then $G_1 \times G_2$ is cyclic.*
(vi) *Let G be a finite abelian group. If G is not cyclic, then there exists a prime p and a subgroup of G isomorphic to $C \times C$, where C is cyclic of order p.*

Proposition 5.1. *If G is a group operating on a set S, and $s \in S$, then the order of the orbit Gs is equal to the index $(G : G_s)$.*

Proposition 5.2. *The number of conjugate subgroups to H is equal to the index of the normalizer of H.*

Proposition 5.3. *There exists a unique homomorphism $\varepsilon : S_n \to \{\pm 1\}$ such that for every transposition τ we have $\varepsilon(\tau) = 1$.*

Theorem 5.4. *If $n \geqq 5$ then S_n is not solvable.*

Theorem 5.5. *If $n \geqq 5$ then the alternating group A_n is simple.*

Lemma 6.1. *Let G be a finite abelian group of order m, let p be a prime number dividing m. Then G has a subgroup of order p.*

Theorem 6.2. *Let G be a finite group and p be a prime number dividing the order of G. Then there exists a p-Sylow subgroup of G.*

Lemma 6.3. *Let H be a p-group acting on a finite set S. Then:*
(i) *The number of fixed points of H is $\equiv \#(S) \bmod p$.*
(ii) *If H has exactly one fixed point, then $\#(S) \equiv 1 \bmod p$.*
(iii) *If $p \mid \#(S)$, then the number of fixed points of H is $\equiv 0 \bmod p$.*

Theorem 6.4. *Let G be a finite group.*

(i) *If H is a p-subgroup of G, then H is contained in some p-Sylow subgroup.*
(ii) *All p-Sylow subgroups are conjugate.*
(iii) *The number of p-Sylow subgroups of G is $\equiv 1 \bmod p$.*

Theorem 6.5. *Let G be a finite p-group. Then G is solvable. If its order is > 1, then G has a non-trivial center.*

Corollary 6.6. *Let G be a p-group which is not of order 1. Then there exists a sequence of subgroups*

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$$

such that G_i is normal in G and G_{i+1}/G_i is cyclic of order p.

Lemma 6.7. *Let G be a finite group and let p be the smallest prime dividing the order of G. Let H be a subgroup of index p. Then H is normal.*

Proposition 6.8. *Let p, q be distinct primes and let G be a group of order pq. Then G is solvable.*

Exercises

1. Show that every group of order $\leqq 5$ is abelian.

   Solution. The trivial group is abelian. According to Proposition 4.1, every group of order 2, 3 and 5 is cyclic, and thus abelian.

   Now, consider a group G of order 4. Suppose there exists $a, b \in G$ such that $ab \neq ba$, and let e be the identity element and c the last element of the group. Then ab can't be equal to a or b, because otherwise we would have $b = e$ or $a = e$ respectively. The same goes for ba. As $ab \neq ba$, we have $ab = e$ and $ba = c$ or the other way around. If $ab = e$ and $ba = c$ then $a = (ab)a = a(ba) = ac$ which is absurd. Thus, G is abelian.

2. 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.

   Solution. Let G be a group of order 4. According to Exercise 1, G is abelian. If G is not cyclic, then according to Proposition 4.3. (vi), G is isomorphic to $C \times C$ where C is a cyclic group of prime order p. Necessarily, $p = 2$.

3. 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.

   Solution. Consider $g \in G$ and $c \in G^c$. Then $xcx^{-1} = (xcx^{-1}c^{-1})c$. Now, we have $xcx^{-1}c^{-1} \in G^c$ and $c \in G^c$, so $xcx^{-1} \in G^c$. Hence, $xG^cx^{-1} \subset G^c$ so G^c is normal.

   Let $f : G \to H$ be a homomorphism, where H is an (additive) abelian group. Then for any $a, b \in G$, we have $f(aba^{-1}b^{-1}) = f(a) + f(b) - f(a) - f(b) = 0$ (because H is abelian). Thus, $G^c \subset \ker f$, which shows that f factors through G/G^c.

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

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

Solution. We have a canonical isomorphism

$$H/(H \cap K) \approx (HK)/K$$

and the result follows by taking cardinalities.

5. **Goursat's Lemma.** Let G, G' be groups, and let H be a subgroup of $G \times G'$ such that the two projections $p_1 : H \to G$ and $p_2 : H \to G'$ 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 $G/N \approx G'/N'$.

   Solution. For any $x \in G$, respectively $x \in G'$, denote by $\overline{x}$ its class in G/N, respectively G/N'. Let

   $$A := \{(\overline{x}, \overline{y}); (x, y) \in H\} \subset G/N \times G'/N'.$$

   First, let us show that A is a graph of a function $\varphi : G/N \to G'/N'$. Let $\overline{x} \in G/N$. As p_1 is surjective, there exists $x \in G$ such that $(x, y) \in H$, so $\overline{x}$ has an image $\overline{y} \in G'/N'$. In addition, this image is unique: if $(\overline{x}, \overline{y}), \left(\overline{x}, \overline{y'}\right) \in A$ then $\left(e, yy'^{-1}\right) \in N'$, so $\overline{yy'^{-1}} = \overline{e}$ and $\overline{y} = \overline{y'}$. Thus, we have defined a function $\varphi : G/N \to G'/N'$, that sends $\overline{x}$ to the unique $\overline{y}$ such that $(x, y) \in H$.

   Now we want to show that φ is an isomorphism. Let $\overline{x}, \overline{x'} \in G/N$. If $\varphi(\overline{x}) = \overline{y}$ and $\varphi\left(\overline{x'}\right) = \overline{y'}$, we have $(x, y), (x', y') \in H$, so $(xx', yy') \in H$. Thus, $\varphi\left(\overline{x}\overline{x'}\right) = \overline{yy'} = \varphi(\overline{x})\varphi\left(\overline{x'}\right)$. This shows that φ is a homomorphism. It is injective: if $\overline{x} \in \ker \varphi$ then $(x, e) \in H$, so $(x, e) \in N$ and $\overline{x} = 0$. Finally, it is surjective: if $\overline{y} \in G'/N'$, then since p_2 is surjective, there exists $x \in G$ such that $(x, y) \in H$, i.e. $\varphi(\overline{x}) = \overline{y}$.

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

   Solution. Let $\operatorname{Inn}(G) = \left\{\boldsymbol{c}_g : x \mapsto gxg^{-1}; g \in G\right\}$ be the group of inner automorphisms. Consider $\boldsymbol{c}_g \in \operatorname{Inn}(G)$ and $\varphi \in \operatorname{Aut}(G)$. Then for all $x \in G$,

   $$\varphi \boldsymbol{c}_g \varphi^{-1}(x) = \varphi\left(g\varphi^{-1}(x)g^{-1}\right) = \varphi(g)x\varphi(g)^{-1}$$

   which shows that $\varphi \boldsymbol{c}_g \varphi^{-1} = \boldsymbol{c}_{\varphi(g)} \in \operatorname{Inn}(G)$. Thus, $\varphi \operatorname{Inn}(G)\varphi^{-1} \subset \operatorname{Inn}(G)$ and $\operatorname{Inn}(G)$ is normal.

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

   Solution. If $\operatorname{Aut}(G)$ is cyclic then the subgroup of inner automorphisms $\operatorname{Inn}(G)$ is also cyclic by Proposition 4.2. We have a homomorphism

   $$\begin{aligned} G \to & \quad \operatorname{Inn}(G) \\ g \mapsto & \left(\boldsymbol{c}_g : x \mapsto gxg^{-1}\right) \end{aligned}$$

   whose kernel is the center $Z(G)$. Thus $G/Z(G) \approx \operatorname{Inn}(G)$ is also cyclic. Consider $g \in G$ such that its class $\overline{g} \in G/Z(G)$ generates $G/Z(G)$.

   Consider $x, y \in G$. We can write $\overline{x} = \overline{g}^k$ and $\overline{y} = \overline{g}^l$ for some integers k, l. In other words, $x = g^k u$ and $y = g^l v$ for some $u, v \in Z(G)$. It follows

   $$xy = g^k u g^l v = g^k g^l uv = g^l g^k uv = g^l v g^k u = yx$$

   so G is abelian.

8. 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

$$H = \bigcup_{x_c} x_c(H \cap [c]H'),$$

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

$$G = \bigcup_{c} \bigcup_{x_c} x_c c H',$$

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

Solution.

a. Every $x \in G$ is in the double coset HxH'. Thus, $G = \bigcup_{x \in G} HxH'$ and it is sufficient to show that two double cosets $HxH' \neq HyH'$ are disjoint. Suppose they are not, and let a be an element in their intersection. We can write $a = h_1 x h_1' = h_2 y h_2'$ with $h_1, h_2 \in H$ and $h_1', h_2' \in H'$. Now, we have

$$HxH' = Hh_1^{-1} a h_1'^{-1} H' = Hh_1^{-1} h_2 y h_2' h_1'^{-1} H' = HyH'$$

which is absurd.

b. There are errors in the indexes of the unions in the exercise statement, at least in my edition (the above statement is correct). For a fixed c, since $H \cap [c]H'$ is a subgroup of H, we indeed have a decomposition into ordinary cosets

$$H = \bigcup_{x_c} x_c(H \cap [c]H')$$

where the union is disjoint. Now,

$$\begin{aligned} G &= \bigcup_{c} HcH' \\ &= \bigcup_{c} \left(\bigcup_{x_c} x_c(H \cap [c]H') \right) cH' \\ &= \bigcup_{c} \bigcup_{x_c} x_c(H \cap [c]H')cH' \end{aligned}$$

and the union is disjoint. It remains to show that for given c and x_c, we have $(H \cap [c]H')cH' = cH'$. If $y \in (H \cap [c]H')cH'$, we can write $y = ch_1c^{-1}ch_2 = ch_1h_2$ with $h_1, h_2 \in H'$. Thus, $(H \cap [c]H')cH' \subset cH'$ and the other inclusion is clear.

9. 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.

Solution.

a. G operates by translation on the set of left cosets G/H. In other words, we have a homomorphism $\varphi : G \to \mathrm{Perm}(G/H)$. Let N be its kernel. Then N is a normal subgroup of G. Moreover, it is contained in H: if $g \in \ker \varphi$ then for all $x \in H$, we have $xH = gxH$ and in particular, $g \in gH = H$. G/N is isomorphic to a subset of $\mathrm{Perm}(G/H)$, thus it is finite, i.e. N is of finite index.

b. By a., there exists two normal subgroups N_1 and N_2 of finite indexes contained in H_1 and H_2 respectively. We know that $(N_1 : N_1 \cap N_2) = (N_1 N_2 : N_2)$. Since N_2 has finite index, $(N_1 N_2 : N_2)$ is finite. Thus, since N_1 is of finite index, $(G : N_1 \cap N_2) = (G : N_1)(N_1 : N_1 \cap N_2)$ is also finite. As $N_1 \cap N_2 \subset H_1 \cap H_2$, the subgroup $H_1 \cap H_2$ also has finite index.

10. 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.

Solution. We define a map between left and right cosets by $\varphi(xH) = Hx^{-1}$. Let's first show that this map is well defined. Suppose $xH = yH$ and let $hx^{-1} \in Hx^{-1}$ (for some $h \in H$). As $x \in yH$, we can write $x = yh'$ for some $h' \in H$. It follows $hx^{-1} = hh'^{-1}y^{-1} \in Hy^{-1}$. Thus $Hx^{-1} \subset Hy^{-1}$ and symetrically, $Hx^{-1} = Hy^{-1}$. So φ is well defined.

φ is obviously surjective, because any right coset Hx is equal to $\varphi(x^{-1}H)$. Finally, it is injective: if $Hx^{-1} = Hy^{-1}$ then $xH = yH$ by the same arguments as above. We have proved that φ is a bijection between left and right cosets. In particular, since H is of finite index, the number of right cosets is also finite and equal to the number of left cosets.

11. Let G be a group, and A a normal abelian subgroup. Show that G/A operates on A by conjugation, and in this manner get a homomorphism of G/A into $\mathrm{Aut}(A)$.

Solution. Consider the operation of G/A on A defined by ${}^{\overline{g}}a = gag^{-1}$. This is well defined: if $\overline{g} = \overline{h}$, then we can write $g = hx$ for some $x \in A$, and since A is abelian, $gag^{-1} = hxax^{-1}h^{-1} = hxx^{-1}ah^{-1} = hah^{-1}$. Moreover, $gag^{-1} \in A$ because A is normal. One can easily see that this indeed defines an operation.

Thus, we have defined a homomorphism $G/A \to \mathrm{Perm}(A)$. In addition, the permutations we just defined are of the form $a \mapsto gag^{-1}$: they are automorphisms, giving us a homomorphism $G/A \to \mathrm{Aut}(A)$.

Semidirect product

12. Let G be a group and let H, N be subgroups with N normal. Let γ_x be conjugation by an element $x \in G$.
   a. Show that $x \mapsto \gamma_x$ induces a homomorphism $f : H \to \mathrm{Aut}(N)$.
   b. If $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if f is trivial, i.e. $f(x) = \mathrm{id}_N$ for all $x \in H$.
   We define G to be the **semidirect product** of H and N if $G = NH$ and $H \cap N = \{e\}$.
   c. Conversely, let N, H be groups, and let $\psi : H \to \mathrm{Aut}(N)$ be a given homomorphism. Construct a semidirect product as follows. Let G be the set of pairs (x, h) with $x \in N$ and $h \in H$. Define the composition law

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_1) x_2, h_1 h_2).$$

   Show that this is a group law, and yields a semidirect product of N and H, identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$.

Solution.

a. For a given $x \in G$, the map $\gamma_x : y \mapsto xyx^{-1}$ induces an automorphism $N \to N$ because N is normal. Moreover, one can easily see that $\gamma_{xy} = \gamma_x \gamma_y$, so $x \mapsto \gamma_x$ induces a homomorphism $H \to \mathrm{Aut}(N)$.

b. The map is obviously surjective by definition of HN. If $xy = x'y'$ then $x'^{-1}x = y'y^{-1} \in H \cap N = \{e\}$, so $(x, y) = (x', y')$. Thus, the map is bijective. It is a morphism if and only if $xx'yy' = xyx'y'$ for all $x, x' \in H$ and $y, y' \in N$, if and only if $x'y = yx'$ for all $x' \in H$ and $y \in N$, if and only if $x'yx'^{-1} = y$ for all $x' \in H$ and $y \in N$, if and only if f is trivial.

c. It is easy to show that the composition law is a group law. In particular, the identity element is $e := (1_N, 1_H)$ and the inverse of (x, h) is $(\psi(h^{-1})x^{-1}, h^{-1})$.

   Identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$, we have $H \cap N = \{e\}$ and $G = NH$. Indeed, for $(x, h) \in G$ we can write $(x, h) = (x, 1)(1, h) \in NH$.

13. a. Let H, N be normal subgroups of a finite group G. Assume that the orders of H, N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \approx HN$.
    b. Let $H_1, ..., H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that

$$H_1 \times ... \times H_r \approx H_1 ... H_r.$$

Example. If the Sylow subgroups of a finite group are normal, then G is the direct product of its Sylow subgroups.
Solution.

a. If $x \in H \cap N$ then the order of x divides the orders of H and N which are coprime, so $x = e$. Thus, $H \cap N = \{e\}$. Now, if $x \in H$ and $y \in N$ then $y^{-1}xy \in H$ since H is normal, hence $y^{-1}xyx^{-1} \in H$. Similarly, $y^{-1}xyx^{-1} \in N$, so $y^{-1}xyx^{-1} = e$, i.e. $xy = yx$. By exercise 12.b, it follows $H \times N \approx HN$.

b. We proceed by induction on r. The case $r = 1$ is trivial and the case $r = 2$ is the previous question. Now, suppose the result is true for $r - 1$, i.e. $H_1 \times ... \times H_{r-1} \approx H_1 ... H_{r-1}$. Then $H_1 \times ... \times H_r \approx H_1 ... H_{r-1} \times H_r$. The orders of $H_1 ... H_{r-1}$ and H_r are relatively prime. Moreover, $H_1 ... H_{r-1}$ is a normal subgroup of G, for if $x_1 ... x_{r-1} \in H_1 ... H_{r-1}$ and $y \in G$ then

$$yx_1 ... x_{r-1}y^{-1} = \underbrace{yx_1y^{-1}}_{\in H_1}\underbrace{yx_2y^{-1}}_{\in H_2} ... \underbrace{yx_{r-1}y^{-1}}_{\in H_{r-1}} \in H_1 ... H_{r-1}.$$

   H_r is also normal, so by the previous question we get $H_1 \times ... \times H_r \approx H_1 ... H_r$.

14. Let G be a finite group and let N be a normal subgroup such that N and G/N have relatively prime orders.
    a. Let H be a subgroup of G having the same order as G/N. Prove that $G = HN$.
    b. Let g be an automorphism of G. Prove that $g(N) = N$.

Solution.

a. As H and N have relatively prime orders, we have $H \cap N = \{e\}$ (see Exercise 13.a.). By Exercise 12.b, we have $\#(HN) = \#(H)\#(N) = \#(G/N)\#(N) = \#(G)$. Thus, $G = HN$.

b. Let $n \in N$. Let ω_1 and ω_2 be the orders of n in N and $\overline{g(n)}$ in G/N respectively. These orders must be relatively prime so by Bézout's theorem, there exists integers u, v such that $u\omega_1 + v\omega_2 = 1$. Moreover, $\overline{g(n^{\omega_2})} = \overline{g(n)}^{\omega_2} = \overline{e}$ so $g(n^{\omega_2}) \in N$. It follows

$$g(n) = g(n^{u\omega_1 + v\omega_2}) = g((n^{\omega_1})^u)g(n^{\omega_2})^v = g(n^{\omega_2})^v \in N$$

which proves that $g(N) \subset N$. Since g is a bijection, $g(N) = N$.

Some operations

15. Let G be a finite group operating on a finite set S with $\#(S) \geqq 2$. 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 $s \in S$.

Solution. Consider the set $A := \{(x, s) \in G \times S; xs = s\}$. On one hand, $A = \bigsqcup_{s \in S} \{x \in G; xs = s\} \times \{s\}$ so $\#(A) = \sum_{s \in S} \#(G_s)$. By proposition 5.1, $\#(G_s) = \frac{\#(G)}{\#(Gs)} = \frac{\#(G)}{\#(S)}$ (the last equality commes from the fact that there is only one orbit, so it is equal to the entire set S). This gives us $\#(A) = \#(G)$.

On the other hand, $A = \bigsqcup_{x \in G} \{x\} \times \{s \in S; xs = s\}$ so $\#(A) = \sum_{x \in G} \#\{s \in S; xs = s\}$. Suppose for the sake of contradiction that every $x \in G$ has a fixed point. Then we have $\#\{s \in S; xs = s\} \geqq 1$ for all $x \in G$, and we even have $\#\{s \in S; xs = s\} = \#S > 1$ for $x = e$. Thus, $\#(A) > \#(G)$, which is absurd and concludes the proof.

16. 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.)

Solution. G operates on the set of subgroups by conjugation. The orbit of H for this operation, which we denote as $G \cdot H$, is the set of conjugates on H. Let A be the union of all the conjugates of H, that is, $A = \bigcup_{F \in G \cdot H} F$. As every conjugate of H has the same cardinality as H, we have

$$\#(A) \leqq \sum_{F \in G \cdot H} \#(H) = \#(G \cdot H)\#(H).$$

If H has at leat two conjugates then this inequality is strict because the identity element is in every conjugate of H, so the above union is not disjoint. Furthermore, $\#(G \cdot H) = \frac{\#G}{\#G_H}$. As $H \subset G_H$, we have $\#(A) < \#(G)$ so G is not the union of all the conjugates of H.

If H has only one conjugate, this conjugate is $H = eHe^{-1}$, so G is not the union of the conjugates of H since H is a proper subgroup.

17. Let X, Y be finite sets and let C be a subset of $X \times Y$. For $x \in X$ let $\varphi(x) =$ number of elements $y \in Y$ such that $(x, y) \in C$. Verify that

$$\#(C) = \sum_{x \in X} \varphi(x).$$

Remark. A subset C as in the above exercise is often called a **correspondence**, and $\varphi(x)$ is the number of elements in Y which correspond to a given element $x \in X$.
Solution. We have $C = \bigsqcup_{x \in X} \{x\} \times \{y \in Y; (x, y) \in C\}$ and the result follows immediately by taking cardinalities.

18. Let S, T be finite sets. Show that $\#\mathrm{Map}(S, T) = (\#T)^{\#(S)}$.

Solution. A function $S \to T$ is defined by choosing the image among the $\#(T)$ elements of T for each of the $\#(S)$ elements in S. Thus the identity is clear.

19. Let G be a finite group operating on a finite set S.
a. For each $s \in S$ show that

$$\sum_{t \in Gs} \frac{1}{\#(Gt)} = 1.$$

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

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

Solution.

a. If $t \in Gs$ then $Gt = Gs$, and the result follows immediately.

b.
$$\begin{aligned}
\frac{1}{\#(G)} \sum_{x \in G} f(x) &= \frac{1}{\#(G)} \sum_{x \in G} \#\{s \in S; xs = s\} \\
&= \frac{1}{\#(G)} \# \bigsqcup_{x \in G} \{x\} \times \{s \in S; xs = s\} \\
&= \frac{1}{\#(G)} \#\{(x,s) \in G \times S; xs = s\} \\
&= \frac{1}{\#(G)} \# \bigsqcup_{s \in S} \{x \in G; xs = s\} \times \{s\} \\
&= \frac{1}{\#(G)} \sum_{s \in S} \#\{x \in G; xs = s\} \\
&= \frac{1}{\#(G)} \sum_{s \in S} \#(G_s) \\
&= \sum_{s \in S} \frac{1}{\#(Gs)} \text{ by proposition 5.1.} \\
&= \sum_{s \in A} \sum_{t \in Gs} \frac{1}{\#(Gt)} \text{ where } A \text{ is a set of representatives of the orbits} \\
&= \sum_{s \in A} 1 \text{ by the previous question} \\
&= \text{number of orbits}
\end{aligned}$$

Troughout, p is a prime number.

20. 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.

    Solution. We have $\#(P) = p^n$ for some integer $n > 0$. P operates on A by conjugation, and the orbit decomposition formula gives

    $$p = \sum_{i \in I} \frac{p^n}{p^{m_i}}$$

    where I is the set of orbits and p^{m_i} is the order of $P_a := \{p \in P; pap^{-1} = a\}$ for some a in the orbit i. But $P_e = P$ so all the m_i must be equal to n (otherwise we would have $\sum_{i \in I} \frac{p^n}{p^{m_i}} > p$). The orbit of e is just $\{e\}$. Consider any other orbit, and any $a \in A$. Then $P_a = P$, i.e. $a \in Z(P)$. But A is a cyclic group of prime order and $a \neq e$, and a is a generator of A, so $A \subset Z(P)$.

21. 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 $P_H = P \cap H$.

22. 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.

Solution. By Theorem 6.4.(i), H is contained in some p-Sylow subgroup P. Let Q be another p-Sylow subgroup of G. By Theorem 6.4.(ii), there exists $a \in G$ such that $Q = aPa^{-1}$. Then, $aHa^{-1} \subset aPa^{-1} = Q$, and $aHa^{-1} = H$ since H is normal. Thus, H is contained in Q.

23. Let P, P' be p-Sylow subgroups of a finite group G.
    a. If $P' \subset N(P)$ (normalizer of P), then $P' = P$.
    b. If $N(P') = N(P)$, then $P' = P$.
    c. We have $N(N(P)) = N(P)$.