Group Theory – Selected Solutions to Exercises

Edward Chernysh

In this document we provide solutions to selected exercises from the assignments of Honours Algebra III (Math 456 at McGill university). The selected exercises have elegant solutions and I suspect many of these questions could appear on the final examination. The topics covered include:

- Abstract groups,
- Cosets and group actions,
- Sylow's theorems,
- Solvable groups,
- Semidirect products,
- Representation theory.

EXERCISE 1. *A Boolean group B is a group such that $g^2 = e$ for every $g \in B$. Prove that every boolean group is Abelian.*

PROOF. We first show that every element is its own inverse. Certainly, if $g = e$ then the result is clear. Otherwise, $gg = e$ so that, by uniqueness, $g^{-1} = g$. If $g, h \in B$ then it follows that

$$(gh) = (gh)^{-1} = h^{-1}g^{-1} = hg.$$

□

EXERCISE 2. *Let $\mathbb{F}$ and $\mathbb{K}$ be finite fields with $\mathbb{F} \subseteq \mathbb{K}$ and let q denote $|\mathbb{F}|$. Establish each of the following:*

(1) $|\mathbb{K}| = q^n$ for some $n \geq 1$;
(2) If $a \in \mathbb{F}$ then $a^q = a$;
(3) If $a \in \mathbb{K}$ satisfies $a^q = a$ then $a \in \mathbb{F}$.

SOLUTION. For the first part, we note that $\mathbb{K}$ forms a vector space over $\mathbb{F}$, indeed this is immediate from the field axioms. Since $\mathbb{K}$ is finite, it is finite dimensional when considered over $\mathbb{F}$. Let $\{b_1, \ldots, b_n\}$ be a basis for $\mathbb{K}$ and note that any

Last updated: December 11, 2017.

vector $u \in \mathbb{K}$ has a unique representation

$$u := \sum_{j=1}^{n} \alpha_j b_j, \quad \alpha_j \in \mathbb{F}.$$

Conversely, any such u determines a vector in $\mathbb{K}$. Since there are exactly q^n possibilities for the n-tuples $(\alpha_1, \ldots, \alpha_n)$, it follows that $|\mathbb{K}| = q^n$. This establishes (1). For the second part, we need only consider $a \in \mathbb{F}^\times$. Since $\mathbb{F}^\times$, as a group, has order $q-1$, it follows that $a^{q-1} = 1$ for every $a \in \mathbb{F}^\times$. This establishes (2).

For the final part, we need only handle the case $a \in \mathbb{K}^\times$ since $\mathbb{F} \cap \mathbb{K} \supset \{0\}$. Noticing that $\mathbb{K}^\times$ has order $q^n - 1$, it becomes clear that $(q-1)$ divides the order of $\mathbb{K}^\times$. Recall that both $\mathbb{F}^\times$ and $\mathbb{K}^\times$ are cyclic groups. Now, if $a^{q-1} = 1$ then $\mathrm{ord}(a) \mid (q-1) \mid (q^n - 1)$. By Lagrange's theorem, $\langle x \rangle$ is the unique subgroup of $\mathbb{K}^\times$ having order $\mathrm{ord}(a)$. But, there also exists a cyclic subgroup of $\mathbb{F}^\times \subseteq \mathbb{K}^\times$ having order precisely $\mathrm{ord}(a)$. By uniqueness in $\mathbb{K}^\times$, we conclude that $\langle a \rangle \subseteq \mathbb{F}^\times$. □

EXERCISE 3. *Let G and H be finite of orders n and m, respectively. Suppose further that $\gcd(n, m) = 1$. Prove that any group homomorphism $G \to H$ is the trivial[1] one.*

SOLUTION. We argue by contradiction. Suppose there exists a non-trivial group homomorphism $f : G \to H$; this means that $\mathrm{Ker}\, f \subsetneq G$. As the kernel of a homomorphism, we know that $\mathrm{Ker}\, f \lhd G$ so that $G/\mathrm{Ker}\, f$ is a well defined quotient group. Also, $G/\mathrm{Ker}\, f$ is non-trivial. However, the first isomorphism theorem gives the congruence

$$G/\mathrm{Ker}\, f \cong f(G) < H.$$

This means that $[G : \mathrm{Ker}\, f]$ is also a divisor of $|H|$. Since $[G : \mathrm{Ker}\, f]$ is non-trivial and also divides the order of G, we have obtained a contradiction. □

EXERCISE 4. *Let G be a finite group and p the minimal prime dividing $|G|$. Show that if H is a subgroup of index p in G, then $H \lhd G$.*

SOLUTION. We may assume without loss of generality that H is a proper subgroup of G. Let $H < G$ have index p. Even if H is not normal in G, we can make sense of G/H as the collection of left cosets of H in G. We consider the action of G upon the elements of G/H by defining an operation

$$\star : G \times G/H, \quad (x, gH) \mapsto xgH. \tag{1}$$

It is easy to check that this is a well defined action. Now, this group action induces a homomorphism

$$\psi : G \to \mathsf{S}_p$$

[1]The trivial homomorphism $G \to H$ is that which takes each $g \in G$ to e_H.

since $[G : H] = p$. Let $N := \operatorname{Ker}\psi$ and note that $N \subseteq H$. Indeed, if $n \in N$ then $\psi(n)$ is the identity permutation. That is, $n(xH) = xH$ for all $xH \in G/H$. In particular, $nH = H$ which is only possible if $n \in H$. Therefore, $N \lhd H$. The first isomorphism theorem states that G/N is isomorphic to a subgroup of S_p. Hence, $[G : N]$ divides both $|G|$ and $p!$. Since $H \neq G$, it follows that $[G : N] = p$. This allows us to write

$$p = [G : N] = \frac{|G|}{|N|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|N|} = [G : H][H : N].$$

This implies that $[H : N] = 1$ whence $H = N$. We are done since N, as the kernel of a homomorphism, is normal in G. □

EXERCISE 5. *Let G be a finite group acting transitively upon a finite set S with more than one element. Show that there exists an element $g \in G$ without any fixed points.*

SOLUTION. We argue by contradiction. As in the CFF, given $g \in G$ we define

$$I(g) := |\{s \in S : g * s = s\}|.$$

Assume every $g \in G$ has at least one fixed point, i.e. $I(g) \geq 1$ for all g. The CFF formula then states that

$$|G| = \sum_{g \in G} I(g) = I(e) + \sum_{g \neq e} I(g) = |S| + \sum_{g \neq e} I(g).$$

However, since $|S| > 1$, this would imply that

$$|G| > 1 + \sum_{g \neq e} I(g) \geq 1 + \sum_{g \neq e} 1 = |G|$$

which is absurd. □

EXERCISE 6. *Let G be a finite group and A a proper subgroup of G. Show that*

$$G \neq \bigcup_{g \in G} gAg^{-1}.$$

SOLUTION. Consider G/A: the left cosets of A in G. As in (1), define an action of G upon G/A by left multiplication. This action is clearly transitive and G/A consists of more than one element. By the previous exercise, we may therefore extract an element $x \in G$ with no fixed points. We claim that $x \notin gAg^{-1}$ for any given $g \in G$. To see this, suppose for a contradiction that $x \in gAg^{-1}$ for any fixed g. Then, $x = gag^{-1}$ for some $a \in A$ whence

$$x * (gA) = (xg)A = (gag^{-1}g)A = gaA = gA$$

which is a contradiction. □

EXERCISE 7. *Let G be a group and $H, K \subseteq G$ two subgroups of finite index. Show that their intersection $H \cap K$ is also a subgroup of finite index.*

SOLUTION. It is easy to verify directly that $H \cap K$ is a subgroup of G; the challenge is to compute $[G : H \cap K]$. First, we define

$$S := (G/H) \times (G/K).$$

Since both H and K have finite index in G, the set S is finite. We now let G act upon S by component-wise left multiplication:

$$g * (xH, xK) \mapsto (gxH, gxK).$$

Noticing that $\mathrm{Stab}(H, K) = H \cap K$, it follows that

$$[G : H \cap K] = |\mathrm{Orb}(H, K)|.$$

Indeed, the proof of the Orbit-Stabilizer theorem gives a bijection

$$G/\operatorname{Stab}(s) \to \mathrm{Orb}(s), \quad \forall s \in S.$$

Therefore, we find that $\mathrm{Orb}(s) = \{(gH, gK) : g \in G\}$ is finite since G/H and G/K are both finite sets. □

EXERCISE 8. *Let G be a simple group of order n. Show that if H is a subgroup of G with $[G : H] = k > 1$ then $k! \geq n$.*

SOLUTION. As we have done multiple times, we define an action of G upon the family of cosets G/H by left multiplication. This then induces a homomorphism $\psi : G \to \mathsf{S}_k$ whose kernel is a normal subgroup of G. Since G is simple, either $\operatorname{Ker}\psi = \{e\}$ or $\operatorname{Ker}\psi = G$. In the latter case, it would follow that $g(xH) = xH$ for all $xH \in G/H$ and $g \in G$. Especially, $gH = H$ so that $g \in H$. Since $[G : H] > 1$ this cannot be, whence ψ must be injective. This injectivity implies that $k! \geq n$, as was required. □

EXERCISE 9. *The class number of a group G is the number of conjugacy classes in G. Prove that if G is a finite group of even class number then $|G|$ must be even.*

SOLUTION. We will show the contrapositive. Suppose that G is a finite group of odd order, we will show that the class number is odd. Since G is the disjoint union of conjugacy classes, we may choose representatives $\{x_1, x_2, \ldots, x_l\}$ such that $G = \bigsqcup_{j=1}^{l} \mathrm{Conj}(x_j)$. Now, by virtue of Orbit-Stabilizer, we have

$$|G| = \left|\mathrm{C}(x_j)\right| \cdot \left|\mathrm{Conj}(x_j)\right|, \quad \forall j \in \{1, \ldots, l\}.$$

Hence, every conjugacy class must have odd cardinality. Finally, since the conjugacy classes are disjoint and an even sum of odd number is even, the class number must be odd. □

EXERCISE 10. *Let A_n be the alternating group on n-letters (for $n \geq 5$) and suppose A_n acts transitively upon a set S of $m > 1$ elements. Deduce that $m \geq n$. (You may use that A_n is simple for $n \geq 5$).*

SOLUTION. The action of A_n upon S grants us a homomorphism $\psi : \mathsf{A}_n \to \mathsf{S}_m$. Since $\operatorname{Ker}\psi$ is a normal subgroup of A_n, either ψ is injective or trivial. If ψ were trivial, then every element of A_n would have a fixed point, which is ridiculous in our case. It follows that $\operatorname{Ker}\psi = \{e\}$. Therefore, $n! \leq 2m!$. We now claim that $n \leq m$. To see this, suppose instead that $m < n$. Then

$$n! = 1 \cdot 2 \cdots m \cdot (m+1) \cdots (n-1) \cdot n > 2m!$$

which is a contradiction. □

EXERCISE 11. *Let G be a finite p-group and $H \neq \{e\}$ a normal subgroup of G.*

(1) Write a class equation for the action of G on H by conjugation;

(2) Show that $H \cap Z(G)$ is non-trivial, where $Z(G)$ the center of G.

SOLUTION. For $(g,h) \in G \times H$ we set $g * h := ghg^{-1}$, which belongs to H (since $H \lhd G$). The orbit of $h \in H$ is simply the set

$$\operatorname{Orb}(h) = \{g * h : g \in G\} = \left\{ghg^{-1} : g \in G\right\} = \operatorname{Conj}(h).$$

It follows that H is the disjoint union of conjugacy classes. Hence, we can choose representatives h_j (finitely many, rather) such that $H = \bigsqcup_j \operatorname{Conj}(h_j)$. Suppose now that $h \in Z(G)$. Then, $\operatorname{Conj}(h) = \left\{ghg^{-1} : g \in G\right\} = \{h\}$. Hence, for $h \in H$:

$$|H| = |H \cap Z(G)| + \sum_{\substack{h \text{ repr.} \\ h \notin Z(G)}} \frac{|G|}{|\mathrm{C}(h)|} \tag{2}$$

where $\mathrm{C}(h) := \left\{g \in G : ghg^{-1} = h\right\}$. This establishes (1). For (2), we note that for $h \notin Z(G)$, the set $\mathrm{C}(h)$ is a proper subgroup of G. Certainly, if $\mathrm{C}(h) = G$ then

$$gh = hg, \quad \forall g \in G$$

so that $h \in Z(G) \cap H$. Hence,

$$|G| \equiv \sum_{\substack{h \text{ repr.} \\ h \notin Z(G)}} \frac{|G|}{|\mathrm{C}(h)|} \equiv 0 \pmod{p}$$

so that $|Z(G) \cap H| \equiv 0 \pmod{p}$ as well. This means that $Z(G) \cap H$ contains at least p elements. □

EXERCISE 12. *Let G be a group of order p, q, r where $p < q < r$ are primes. This group G has a normal Sylow subgroup and, moreover, G is solvable.*

SOLUTION. Let n_p denote the number of p-Sylow subgroups in G and likewise for q and q; we shall first show that at least one of these is 1. Suppose, by way of contradiction, that $n_{p,q,r} > 1$. We know that $n_r \mid pq$ and $n_r \equiv 1 \pmod{r}$. Thus,

$$n_r = 1 + kr, \quad k \geq 1.$$

If $n_r = p$ then $p = 1 + kr > r$, which is absurd. Likewise, $n_r \neq q$. This means that $n_r = pq$. Applying Sylow's theorems to n_q, we have that

$$n_q \equiv 1 \pmod{q} \quad \text{and} \quad n_q \mid pr.$$

Thus, $n_q = 1 + kq$ for $k \geq 1$ (if $n_q = 1$ then the q-Sylow subgroup is normal). Now, $n_q \nmid p$ for, otherwise, we would have

$$p = n_q = 1 + kq > q$$

which is absurd. This means that $n_q \geq r$ and, likewise, $n_p \geq q$. We note that two distinct subgroups of prime order intersect only at the identity (by Lagrange's theorem). Furthermore, two subgroups whose orders are distinct primes can only intersect at the identity (once again, by Lagrange's theorem). Combining all these facts, it follows from the fact that the identity belongs to each Sylow subgroup that:

$$\begin{aligned} prq = |G| \geq pq(r-1) + r(q-1) + q(p-1) &= pqr + rq - r - q \\ &> pqr. \end{aligned}$$

This is a contradiction. □

EXERCISE 13. *Let G be a finite group and $H \lhd G$. Suppose P is a p-Sylow subgroup of G, for some prime p. Prove that $H \cap P$ is a maximal p-subgroup of H (where we exceptionally say that $\{e\}$ is a p-subgroup). Prove also that HP/H is a p-Sylow subgroup of G/H.*

SOLUTION. Obviously $H \cap P$ is a p-subgroup (with a possible exceptional technicality). We now show that $H \cap P$ is a maximal p-subgroup of H. Certainly, let K be a maximal p-subgroup of G that contains $H \cap P$. Let, also, K_1 be a maximal p-subgroup of G with $K_1 \supseteq K$. From the proof of Sylow's theorems we know that $P = gK_1g^{-1}$ whence it follows that

$$P \cap H = H \cap \left[gK_1g^{-1}\right] \supseteq H \cap \left[gKg^{-1}\right] = [gHg^{-1}] \cap \left[gKg^{-1}\right].$$

Clearly, this means that

$$P \cap H \supseteq g\left[H \cap K\right]g^{-1} = gKg^{-1}.$$

Since $P \cap H \subseteq K$ we have $|P \cap H| \leq |K|$. But the above also gives

$$|P \cap H| \geq |K|.$$

Thus, $P \cap H = K$ which shows that $P \cap H$ is maximal. We now argue that HP/H is a p-Sylow subgroup of G/H. Suppose $|G| = p^r m$ and $|H| = p^a n$, where $\gcd(p, n) = \gcd(p, m) = 1$. By Lagrange's theorem, $a \leq r$ and $|G/H| = p^{r-a} d$ where $d = n/m$. Now, HP/H has order[2]

$$\frac{|P|\,|H| \,/\, |H \cap P|}{|H|} = \frac{|P|}{|P \cap H|}.$$

By the first part (the fact that $H \cap P$ is a p-Sylow subgroup of H), we must have that $|H \cap P| = p^a$. This shows, by virtue of the above equation, that

$$|HP/H| = \frac{|P|}{|P \cap H|} = p^{r-a}.$$

□

EXERCISE 14. *Let $n \in \mathbb{N}$ and $a \in \mathbb{N}$ such that $\gcd(n, a) = 1$. Prove that the map defined by*

$$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto ax$$

is an automorphism of $\mathbb{Z}/n\mathbb{Z}$. Deduce from this that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

SOLUTION. We begin by showing that f is indeed an automorphism of $\mathbb{Z}/n\mathbb{Z}$. Clearly, if $x, y \in \mathbb{Z}/n\mathbb{Z}$ then

$$f(x + y) = a(x + y) = ax + ay = f(x) + f(y);$$

hence f is a group homomorphism. Now, f is injective since $f(x) = f(y)$ if and only if $ax = ay$. Since $\gcd(a, n) = 1$, a is invertible. This means that $x = y$. Since f is an injective endomorphism of a finite set, it must also be an automorphism.

Now, let $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. We will show that f is of the form $f(x) = ax$ for some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. Certainly, by additivity we obtain that

$$f(x) = f(1 + 1 \cdots + 1) = xf(1).$$

Set $a := f(1)$ so that $f(x) = xa$ and $f(1) = a$. Now, since f is an automorphism:

$$n = \mathrm{ord}(1) = \mathrm{ord}(f(1)) = \mathrm{ord}(a).$$

By the formula for generators of a cyclic group, we must then have $\gcd(a, n) = 1$. More precisely, this follows from the fact that 1 generates $\mathbb{Z}/n\mathbb{Z}$ together with the equation

$$\mathrm{ord}(a) = \mathrm{ord}(1^a) = \frac{n}{\gcd(a, n)}.$$

Thus, $f = xa$ for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We now define

$$\Psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad a \mapsto f_a$$

[2]Note that this also follows from the second isomorphism theorem for groups.

where f_a is the automorphism of $\mathbb{Z}/n\mathbb{Z}$ given by $f_a(x) = f(x) = ax$. Let now $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, then

$$\Psi(ab) = f_{ab} = (f_a \circ f_b).$$

This shows that Ψ is a group homomorphism. We have already checked that Ψ is surjective, and so it remains only to verify injectivity. Assume $\Psi(a) = \Psi(b)$ whence $f_a = f_b$. This means that $f_a(1) = f_b(1)$ so that $a = b$. □

EXERCISE 15. *Find two non-isomorphic groups with the same composition factors where only one of the groups is Abelian.*

SOLUTION. Consider S_3 which is of order 6 and $\mathbb{Z}/6\mathbb{Z}$. The first group is non-Abelian while the second clearly is. Hence, they cannot be isomorphic. Moreover, the composition factors of each group will be orders 2 and 3. Since all groups of prime order are isomorphic, we are done. □

EXERCISE 16. *Let $G = N \rtimes_\phi B$. Prove that G is Abelian if and only if N and B are Abelian and ϕ is the trivial homomorphism.*

SOLUTION. One direction is quite easy: if N and B are Abelian and ϕ is the trivial homomorphism then $N \rtimes_\phi B \cong N \times B$, which is Abelian. Conversely, suppose that $N \rtimes_\phi B$ is Abelian. Then, for all $(n_1, b_1), (n_2, b_2) \in G$:

$$(n_1\phi_{b_1}(n_2), b_1b_2) = (n_1, b_1)(n_2, b_2) = (n_2, b_2)(n_1, b_1) = (n_2\phi_{b_2}(n_1), b_2b_1).$$

This clearly implies that B is Abelian. By taking $b_1 = b_2 = e$ we obtain $n_1n_2 = n_2n_1$ whence it follows that N is also Abelian. Now, we need only check that ϕ must be the trivial homomorphism $B \to \mathrm{Aut}(N)$. This is done by letting $n = n_1 = n_2$ be arbitrary and using the above to obtain

$$n_1\phi_{b_1}(n_2) = n_2\phi_{b_2}(n_1) \implies \phi_{b_1}(n) = \phi_{b_2}(n).$$

This means that $\phi_{b_1} \equiv \phi_{b_2}$ for all $b_1, b_2 \in B$. In particular, $\phi_b \equiv \phi_e$ for all $b \in B$ whence it follows that ϕ is the trivial homomorphism. □

EXERCISE 17. *Let G be a group and (ρ, V) an irreducible finite dimensional linear representation of G. Then, as vector spaces,*

$$\mathrm{End}_G(V) \cong \mathbb{C}.$$

(Note: this is the key, final step in the proof of Schur's lemma).

SOLUTION. Let $T \in \mathrm{End}_G(V)$; then T is an endomorphism of V that "commutes" with $\rho(g)$. More precisely,

$$T \circ \rho(g) \equiv \rho(g) \circ T, \quad \forall g \in G.$$

Now let $\lambda \in \mathbb{C}$ be an eigenvalue of T and denote by V_λ the corresponding (non-zero) eigenspace. We first argue that $(\rho_{|V_\lambda}, V_\lambda)$ is a sub-representation of (ρ, V). Certainly, let $u \in V_\lambda$ and observe that for each $g \in G$:

$$(T \circ \rho(g))(u) = (\rho(g) \circ T)(u) = \rho(g)(\lambda u) = \lambda \rho(g)(u).$$

It follows that $\rho(g)(u) \in V_\lambda$ for every $u \in V_\lambda$, i.e. $\rho(g)(V_\lambda) \subseteq V_\lambda$. Since (ρ, V) is irreducible and the eigenspace is non-trivial, we must have $V_\lambda = V$. This shows that every element of $\mathrm{End}_G(V)$ is λI, for some $\lambda \in \mathbb{C}$. Conversely, if λ is any complex number, the map $T := \lambda I$ belongs to $\mathrm{End}_G(V)$. Indeed, for every $g \in G$ and $v \in V$:

$$(T \circ \rho(g))(v) = (\lambda I)(\rho(g)(v) = \lambda \rho(g)(v) = \rho(g)(\lambda v) = (\rho(g) \circ T)(v).$$

This means that the mapping $\Gamma : \mathrm{End}_G(V) \to \mathbb{C}$ given by which takes T to the associated[3] λ is a well defined bijection. To see that Γ is an isomorphism of vector spaces, we need only note that for $T, S \in \mathrm{End}_G(V)$ there exist $\lambda_1, \lambda_2 \in \mathbb{C}$ such that $T = \lambda_1 I$ and $\lambda_2 I$ whence

$$\Gamma(T + S) = \Gamma((\lambda_1 + \lambda_2)I) = (\lambda_1 + \lambda_2) = \Gamma(T) + \Gamma(S).$$

This completes the proof. □

EXERCISE 18. *Let G be a finite group, (ρ, V) an irreducible finite dimensional linear representation of G, and fix $z \in Z(G)$. Show that*

$$T := \rho(z) : V \to V$$

is a scalar multiple of the identity.

SOLUTION. From the solution to the previous exercise, it suffices to check that T is an element of $\mathrm{End}_G(V)$. To this end, let $g \in G$ be given and fix $v \in V$. Then,

$$\begin{aligned}(T \circ \rho(g))(v) = (\rho(z) \circ \rho(g))(v) &= \rho(zg)(v) \\ &= \rho(gz)(v) \\ &= (\rho(g) \circ \rho(z))(v) \\ &= (\rho(g) \circ T)(v).\end{aligned}$$

As $v \in V$ was taken arbitrarily, it follows that $(T \circ \rho(g)) \equiv (\rho(g) \circ T)$ for each $g \in G$. This means that $T \in \mathrm{End}_G(V)$ so that $T = \lambda I$, where $\lambda \in \mathbb{C}$ and the eigenvalue of T. □

[3]We have shown that every $T \in \mathrm{End}_G(V)$ is of the form λI for some $\lambda \in \mathbb{C}$. This λ can then be associated to T.