Homework 3
Algebra

Joshua Ruiter

April 7, 2018

Lemma 0.1 (for Exercise 1a)**.** *Let $\mathbb{Z}_n$ be the finite cyclic group of order n. Then* $\mathrm{Aut}(\mathbb{Z}_n)$ *has order $\phi(n)$ (ϕ is the Euler totient function).*

Proof. First we show that $\mathrm{Aut}(\mathbb{Z}_n)$ has order $\phi(n)$. By Proposition 4.3(ii) (Lang), the generators of $\mathbb{Z}_n$ are the positive integers a less than n that are relatively prime to n. By 4.3(iii) (Lang), for any such a relatively prime to n, there is an automorphism $\gamma_a : \mathbb{Z}_n \to \mathbb{Z}_n$ that maps 1 onto a. This determines γ_a completely. Thus there are exactly $\phi(n)$ automorphisms of $\mathbb{Z}_n$. □

Corollary 0.2 (for Exercise 1a)**.** *Let $\mathbb{Z}_p$ be a cylic group of prime order. Then* $\mathrm{Aut}(\mathbb{Z}_p)$ *has order $p - 1$.*

Proof. By above, $\mathrm{Aut}(\mathbb{Z}_p)$ has order $\phi(p)$. $\phi(p)$ counts the number of positive integers less than p that are coprime with p. As p is prime, this is all the numbers $1, 2, \dots p - 1$. Thus $\phi(p) = p - 1$. □

Lemma 0.3 (for Exercise 1a)**.** *Let G, H be finite groups such that* $\gcd(|G|, |H|) = 1$*. Then any group homomorphism $\psi : G \to H$ is trivial, that is, $\phi(g) = e_H$ for $g \in G$.*

Proof. We know that $\psi(G)$ is a subgroup of H, so by Lagrange's Theorem, $|\psi(G)|$ divides $|H|$. We also know that $\ker \psi$ is a normal subgruop of G, so by the first isomorphism theorem, $G/\ker \psi \cong \psi(G)$ so $|\psi(G)| = |G|/|\ker \psi|$ so $|\psi(G)|$ divides $|G|$. Since $\gcd(|G|, |H|) = 1$ by hypothesis and $|\psi(G)|$ divides both, it must be one. Thus $\psi(G) = \{e\}$. □

Lemma 0.4. *Let G be a group, and let P be a p-subgroup and Q be a q-subgroup, where p, q are distinct primes. Then $P \cap Q = \{e\}$.*

Proof. Any $x \in P$ has order divisible by p, except the identity. Any $y \in Q$ has order divisible by q, except the identity. Since p, q are primes, this means that $P \cap Q = \{e\}$. □

Lemma 0.5 (for Exercise 1a)**.** *Let G, H be cyclic groups of coprime order. Then $G \times H$ is cyclic.*

Proof. Let g be a generator for G and h a generator for H. We claim that (g, h) is a generator for $G \times H$. We know that the order of (g, h) divides pq, the order of $G \times H$. Hence it has order $1, p, q$, or pq. It can't have order 1. It doesn't have order p since h has order q and p, q are coprime. Similarly, it doesn't have order q. Thus (h, g) has order pq, so it generates $G \times H$. □

Proposition 0.6 (Exercise 1a)**.** *Let G be a group of order pq where p, q are primes such that $p < q$ and $q \not\equiv 1 \bmod p$. Then G is cyclic.*

Proof. Let H_q be the Sylow subgroup of order q. Then H_q is normal by Lemma 6.7 (Lang). Let H_p be the Sylow subgroup of order p. Then H_p operates by conjugation on H_q, which gives us a homomorphism $\psi : H_p \to \mathrm{Aut}(H_q)$ (where $\psi(x)$ is the conjugation $y \mapsto xyx^{-1}$). We know that H_p has order p, and by our lemma, $\mathrm{Aut}(H_q)$ has order $q-1$.

By hypothesis, $q \not\equiv 1 \bmod p$, so p does not divide $q-1$. Since p is prime, this means that $\gcd(p, q-1) = 1$. Thus by our second lemma, ψ is the trivial homomorphism. This implies that for $x \in H_p, y \in H_q$, we have $xyx^{-1} = y \implies xy = yx$. Finally, we also have $P \cap Q = \{e\}$, so by Proposition 2.1 (Lang), $G \cong P \times Q$. By our last lemma, the product of cyclic groups of coprime order is cyclic, so G is cyclic of order pq. □

Lemma 0.7 (for Exercise 1b)**.** *Let N, H be groups and $\psi : H \to \mathrm{Aut}(N)$. Then the semidirect product $N \rtimes_\psi H$ is abelian if and only if N, H are both abelian and ψ is the trivial homomorphism.*

Proof. First suppose that N, H are abelian and ψ is trivial, that is, $\psi(h) = \mathrm{Id}_N$ for $h \in H$. Then the product in $N \rtimes H$ is given by

$$(n_1, h_1)(n_2, h_2) = (n_1\psi(h_1)n_2, h_1h_2) = (n_1n_2, h_1h_2)$$

so $N \rtimes H \cong N \oplus H$, hence $N \rtimes H$ is abelian.

Now supppose that $N \rtimes H$ is abelian. Then every subgroup is abelian, so by identifying N, H with the subgroups

$$N \cong \{(n, e_H) : n \in N\} \subset N \rtimes H$$
$$H \cong \{(e_N, h) : h \in H\} \subset N \rtimes H$$

we see that N, H must be abelian. As H is normal, ψ must be trivial by Exercise 12(b) from Homework 2. □

Proposition 0.8 (Exercise 1b)**.** *Let G be a group of order pq where p, q are primes such that $p < q$ and $q \equiv 1 \bmod p$. Then there exists a nonabelian group of order pq.*

Proof. We repeat the first paragraph of the proof for part (a) since it still holds. Let H_q, H_p be Sylow subgroups of order q, p. Then H_q is normal, and H_p operates by conjugation on H_q, which gives a homomorphism $\psi : H_p \to \mathrm{Aut}(H_q)$. H_p has order p, and $\mathrm{Aut}(H_q)$ has order $q-1$.

Now the proof diverges. By hypothesis, $p|(q-1)$. Since $\mathrm{Aut}(H_q)$ has order $q-1$, by Cauchy's Theorem there exists an element of $y \in \mathrm{Aut}(H_q)$ of order p. Let x be a generator of H_p. Then we define

$$\phi : H_p \to \mathrm{Aut}(H_q)$$
$$\phi(x) = y$$

and we extend ϕ to a homomorphism by defining $\phi(x^k) = \phi(x)^k = y^k$. Thus ϕ is a nontrivial homomorphism, so by the above lemma, $H_q \rtimes_\phi H_p$ is nonabelian. Thus $H_q \rtimes_\phi H_p$ is a nonabelian group of order pq. □

Lemma 0.9 (for Exercise 2)**.** *Abelian groups are solvable.*

Proof. Let G be an abelian group. Then $G \supset \{e\}$ is a normal abelian tower, so G is solvable. □

Corollary 0.10 (for Exercise 2)**.** *Cyclic groups are solvable.*

Proof. Every cyclic group is abelian, and hence solvable by the above lemma. □

Lemma 0.11 (for Exercises 2,28)**.** *Let P, P' be p-Sylow subgroups of G with $|P| = |P'| = p$. Then $P = P'$ or $P \cap P' = \{e\}$.*

Proof. As P, P' are subgroups, their intersection $P \cap P'$ is a subgroup. It is a subgroup of P, so it has order 1 or p. If it has order p, then $P = P'$. Otherwise, the intersection must be $\{e\}$. □

Lemma 0.12. *Let G be a group of order pq where p, q are distinct primes and $p < q$. Then G has a normal subgroup of order q.*

Proof. Let n_q be the number of Sylow q-subgroups of G. We know that n_q divides $|G|$ and $n_q \equiv 1 \bmod q$, so if $n_q \neq 1$ then $n_q > q > p$. But then $n_q = |G|$, which is impossible. Thus $n_q = 1$, thus any Sylow q-subgroup an unique. (We know a Sylow q-subgroup exists by the first Sylow Theorem.) □

Proposition 0.13 (Exercise 21)**.** *Let G be a finite group and H a subgroup. Let P_H be a p-Sylow subgroup of H. Then there exists a p-Sylow subgroup P of G such that $P_H = P \cap H$.*

Proof. Since P_H is a p-Sylow subgroup of H, it is a p-subgroup of G, so by the first Sylow theorem there exists a p-Sylow subgroup P of G such that $P_H \subset P$. Then we have $P_H \subset P$ and $P_H \subset H$, so $P_H \subset P \cap H$. As a result, $|P_H| \leq |P \cap H|$.

The intersection of subgroups is a subgroup, so $P \cap H$ is a subgroup of H and of P. By Lagrange's Theorem, since $P \cap H$ is a subgroup of P it is a p-group, and since it is a subgroup of H its order is no more than the order of P_H, since P_H is a p-Sylow. That is, $|P \cap H| \leq |P_H|$. Since we have $|P_H| \leq |P \cap H|$ from before, we then have $|P_H| = |P \cap H|$. Any subset of a finite set with the same order must be the whole set, so $P_H = P \cap H$. □

Proposition 0.14 (Exercise 23a)**.** *Let P, P' be p-Sylow subgroups of a finite group G, such that $P' \subset N(P)$. Then $P' = P$. Consequently, P is the unique p-Sylow subgroup of $N(P)$.*

Proof. Let P have order p^k, that is, let k be the highest power of p dividing $|G|$. We know that P is normal in $N(P)$. Since $P' \subset N(H)$, we know that PP' is a subgroup of $N(P)$. By the second isomorphism theorem,

$$|PP'| = \frac{|P||P'|}{|P \cap P'|} \implies |PP'||P \cap P'| = p^{2k}$$

from this we know that PP' and $P \cap P'$ are both p-groups. We know that $P \subset PP'$ so $|PP'|$ is at least p^k. Since k is the highest power of p dividing G and PP' is a subgroup of G, $|PP'|$ cannot be greater than p^k, so we have $|PP'| = p^k$. Thus $|P \cap P'| = p^k$. Since P has order p^k and $P \subset P \cap P'$, it must be that $P \cap P' = P$. Thus $P \subset P'$. Since P' also has order p^k, it similarly follows that $P' \subset P$. Thus $P = P'$. From this it follows that any p-Sylow subgroup of $N(P)$ is equal to P, so P is the unique p-Sylow subgroup of $N(P)$. □

Proposition 0.15 (Exercise 23b)**.** *Let G be a finite group and P, P' be p-Sylow subgroups such that $N(P') = N(P)$. Then $P' = P$.*

Proof. Suppose that $N(P') = N(P)$. We know that $P' \subset N(P')$, so $P' \subset N(P)$. Then by part (a), $P = P'$. □

Proposition 0.16 (Exercise 23c)**.** *Let G be a finite group and P be a p-Sylow subgroups. Then $N(N(P)) = N(P)$.*

Proof. We kow that $P \subset N(P) \subset N(N(P))$, so we just need to show that $N(N(P)) \subset N(P)$. Let $x \in N(N(P))$. First note that $xN(P)x^{-1} = N(P)$ since $N(P)$ is a normal subgroup of G. Then $xPx^{-1} \subset xN(P)x^{-1} = N(P)$ so xPx^{-1} is a p-Sylow subgroup of $N(P)$. By part (a), P is the unique p-Sylow subgroup of $N(P)$, so $xPx^{-1} = P$. Thus $x \in N(P)$. Thus we have shown that $N(N(P)) \subset N(P)$, so we have equality. □

Lemma 0.17 (for Exercise 28, repeated from Homework 1)**.** *Let G be a group such that $G/Z(G)$ is cyclic. Then G is abelian.*

Proof. Since $G/Z(G)$ is cyclic, it can be written as $\langle xZ(G)\rangle$ for some $x \in G$. Let $g \in G$. Then $gZ(G) = x^n Z(G)$ for some n, and so $x^{-n}g \in Z(G)$. Let $z = x^{-n}g$, then $g = x^n z$. Thus every element of G can be written in the form $x^k z$ for some $z \in Z$. Let $g, h \in H$, and write them as $g = x^n z_1, h = x^m z_2$. Then, noting that z_1, z_2 commute with everything in G and x^m commutes with x^n,

$$gh = x^n z_1 x^m z_2 = x^n x^m z_1 z_2 = x^m x^n z_2 z_1 = x^m z_2 x^n z_1 = hg$$

Thus G is abelian. □

Lemma 0.18 (for Exercise 28)**.** *Let p be a prime and let G be a group of order p^2. Then G is abelian.*

Proof. Since G is a p-group, it has non-trivial center, so $|Z(G)| = p$ or $|Z(G)| = p^2$. If the center has order p^2 then G is abelian. If $|Z(G)| = p$ then $|G/Z(G)| = |G|/|Z(G)| = p^2/p = p$, so $G/Z(G)$ has prime order, so it is cyclic. Then G is abelian by the above lemma. □

Lemma 0.19 (for Exercise 28)**.** *Let G be a group and p a prime dividing the order of G. Let n_p be the number of p-Sylow subgroups of G. Then $n_p = [G : N(P)]$. Consequently, n_p divides G, and p does not divide n_p.*

Proof. Let G be a group and let $\mathrm{Syl}_p(G)$ be the set of p-Sylow subgroups of G. (We have $n_p = \mathrm{Syl}_p(G)$ by definition.) Let G act on $\mathrm{Syl}_p(G)$ by conjugation, and let $P \in \mathrm{Syl}_p(G)$. By the second Sylow theorem, the orbit of P is $\mathrm{Syl}_p(G)$. Then by the orbit-stabilizer theorem,

$$|\operatorname{Syl}_p(G)| = |\operatorname{orb}_G(P)| = |G|/|\operatorname{stab}_G(P)|$$

The stabilizer of P is the set

$$\{g \in G : gPg^{-1} = P\}$$

which is precisely the normalizer of P, $N_G(P)$. The normalizer of any subgroup is a normal subgroup, so

$$n_p = |\operatorname{Syl}_p(G)| = |G|/|N_G(P)| = [G : N_G(P)]$$

Then by Lagrange's Theorem, n_p divides $|G|$. We know that P is a subgroup of $N_G(P)$, so p^k divides $|N_G(P)|$. Thus n_p divides $|G|/p^k$. Since P is a p-Sylow subgroup of G, no higher power of p divides $|G|$, so $|G|/p^k$ is not divisible by p. Thus n_p is not divisible by p. □

Lemma 0.20 (repeated from earlier in this document)**.** *Let P, P' be p-Sylow subgroups of G with $|P| = |P'| = p$. Then $P = P'$ or $P \cap P' = \{e\}$.*

Proposition 0.21 (Exercise 28)**.** *Let p, q be distinct primes and let G be a group of order p^2q. Then G is solvable and it has a normal Sylow subgroup.*

Proof. Let P be a p-Sylow subgroup (of order p^2) and Q be a q-Sylow subgroup (of order q). First we claim that one of P, Q must be normal. Let n_p be the number of p-Sylow subgroups and n_q be the number of q-Sylow subgroups. If $n_p = 1$ then P is normal, and if $n_q = 1$ then Q is normal, so assume that neither is equal to one.

By our lemmas, n_p divides $|G| = p^2q$ but is not divisible by p, so $n_p = 1$ or $n_p = q$, but we already ruled out $n_p = 1$. By the third Sylow theorem, $n_p = q \equiv 1 \bmod p$, and since $q \neq 1$, this implies $q = pk + 1$ for $k \geq 1$, so $q > p$. Also by our lemmas, n_q divides p^2q but is not divisible by q, so $n_q = p$ or $n_q = p^2$. Again by the third Sylow theorem, $n_q \equiv 1 \bmod q$. Since $q > p$, this rules out $n_q = p$, so we have $n_q = p^2$.

Using Lagrange's theorem, every element of G has order $1, p, p^2$, or q. An element of order q must be contained in a q-Sylow subgroup, so there are $n_q(q-1) = p^2(q-1)$ elements of order q (note that distinct q-Sylow subgroups of order q intersect only in the identity by a previous lemma). Any remaining element of G has order dividing p^2, so there are $p^2q - p^2(q-1) = p^2$ elements of order dividing p^2. Since we have the p-Sylow subgroup P which has p^2 elements, this can be the only p-Sylow subgroup. Thus $n_p = 1$, which contradicts our earlier assumption that $n_p \neq 1$. Thus one of P, Q is normal.

If P is normal, then

$$G \supset P \supset \{e\}$$

is a normal tower. We know that $|G/P| = p^2q/p^2 = q$ so $|G/P|$ is cyclic and hence abelian, and since $|P| = p^2$ we know that P is abelian, so it is a abelian tower. On the other hand, if Q is normal, then

$$G \supset Q \supset \{e\}$$

is a normal tower, and it is also abelian, since $|G/Q| = p^2$ so G/Q is abelian and $|Q| = q$ so Q is cyclic and hence abelian. Hence G is solvable. □

Lemma 0.22 (for Exercise 36)**.** *Let $\sigma \in S_n$, where $\sigma = (a_1\ a_2 \dots a_k)$. Then for any $\tau \in S_n$, we have*

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2) \dots \tau(a_k))$$

so conjugation in S_n preserves cycle structure. Conversely, for any $\sigma, \tau \in S_n$ with the same cycle structure, that is, if

$$\sigma = (a_1\ a_2 \dots a_k)$$
$$\tau = (b_1\ b_2 \dots b_k)$$

then σ and τ are conjugate.

Proof. We need to show that $\tau\sigma\tau^{-1}(\tau(a_i)) = \tau(a_{i+1 \bmod k})$. By definition, $\sigma(a_i) = \sigma(a_{i+1 \bmod k})$. Thus

$$\tau\sigma\tau^{-1}\tau(a_i) = \tau\sigma(a_i) = \tau(a_{i+1 \bmod k})$$

We also note that $\tau\sigma\tau^{-1}$ leaves fixed any element that σ fixes.

For the converse, let $\sigma = (a_1 \dots a_k), \tau = (b_1 \dots b_k)$. Define a permutation α by $\alpha(a_i) = b_i$, and $\alpha(x) = x$ for $x \neq a_i$. Then

$$\alpha\sigma\alpha^{-1} = (\alpha(a_1) \dots \alpha(a_k)) = (b_1 \dots b_k) = \tau$$

so σ, τ are conjugate in S_n. □

Proposition 0.23 (Exercise 36)**.** *The conjugacy class of $\sigma = (1\ 2\ 3 \dots n) \in S_n$ has $(n-1)!$ elements. Consequently, the centralizer of σ is precisely the cyclic subgroup generated by σ.*

Proof. By the lemma above, an element τ of S_n is conjugate to σ if and only if it is an n-cycle. An τ must be of the form $(a_1 \dots a_n)$ where all the a_i are distinct. In particular, some a_i must be equal to n. We can then rewrite τ as $\tau = (n\ a_2 \dots a_k)$.

We claim that a_2 can be anything in $\{1, \dots n-1\}$ and that all such choices give distinct n-cycles. Suppose $x, y \in \{1, \dots n-1\}$. Then $(1\ x \dots a_k) \neq (1\ y \dots a_k)$ since the first maps 1 to x and the second maps 1 to y. By a similar reasoning, once a choice for a_2 is fixed, there are $n-2$ choices for a_3, et cetera. Hence there are $(n-1)(n-2)\dots(2)(1) = (n-1)!$ distinct n-cycles. Thus the conjugacy class of σ has $(n-1)!$ elements.

Finally, the index of the centralizer of σ is equal to the size of the conjugacy class, so

$$(n-1)! = [S_n : C(\sigma)] = |S_n|/|C(\sigma)| = n!/|C(\sigma)|$$

which gives us $|C(\sigma)| = n$. Since the cyclic subgroup generated by σ has n elements and any subgroup containing σ contains that cyclic subgroup, that cyclic subgroup is all of $C(\sigma)$. Thus $C(\sigma) = \langle\sigma\rangle$. □

Proposition 0.24 (Exercise 38a)**.** *The symmetric group S_n is generated by the transpositions $(12), (13), (14), \dots (1n)$.*

Proof. We can write any $\sigma \in S_n$ as a product of disjoint cycles,

$$\sigma = (a_1 \dots a_k)(b_1 \dots b_j)(c_1 \dots c_m)\dots$$

We just need to show that any disjoint cycle can be written as a product of $(12), (13), \dots (1n)$. We can write a cycle $(a_1 \dots a_k)$ as

$$(a_1 \dots a_k) = (a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_3)(a_1 a_2)$$

We can write each of the terms in the above RHS as

$$(a_1\ a_j) = (1\ a_1)(1\ a_j)(1\ a_1)$$

as long as $a_1 \neq 1$ and $a_j \neq 1$. But if $a_1 = 1$ or $a_j = 1$, then $(a_1\ a_j)$ is already one of our generators. Thus we can write $(a_1 \dots a_k)$ as product of our generators, and hence we can write σ as a product of our generators. □

Proposition 0.25 (Exercise 38b)**.** *The symmetric group S_n is generated by the transpositions* $(12), (23), (34), \dots (n-1, n)$.

Proof. We will show that these transpositions generate the transpositions $(12), (13), \dots (1n)$, then use part (a). Let H be the subgroup generated by $(12), (23), \dots (n-1, n)$. Note that

$$\begin{aligned}(12)(23)(12) &= (13)\\ (13)(34)(13) &= (14)\\ &\vdots\\ (1, n-1)(n-1, n)(1, n-1) &= (1n)\end{aligned}$$

so $(13), (14), \dots (1n) \in H$. Thus H contains the generating set $(12), (13), \dots (1n)$ so by part (a) H is S_n. □

Proposition 0.26 (Exercise 38c)**.** *S_n is generated by the cycles* $(12), (123 \dots n)$.

Proof. We compute

$$\begin{aligned}(123\dots n)(12)(123\dots n)^{-1} &= (123\dots n)(12)(n, n-1\dots 321) = (23)\\ (123\dots n)(23)(123\dots n)^{-1} &= (123\dots n)(23)(n, n-1\dots 321) = (34)\\ &\vdots\\ (123\dots n)(a, a+1)(123\dots n)^{-1} &= (123\dots n)(a, a+1)(n, n-1\dots 321) = (a+1, a+2)\end{aligned}$$

where $a+1$ and $a+2$ are understood to be addition modulo n. Hence any subgroup containing the two cycles $(12), (123 \dots n)$ contains all the transpositions $(12), (23), \dots (n-1, n)$. As shown in part (b), these transpositions generate S_n, so the claim is proven. □

Proposition 0.27 (Exercise 38d)**.** *If n is prime, and τ is the tranposition $(a\ b)$ (where $a \neq b$), then τ and $\sigma = (1\ 2 \dots n)$ generate S_n.*

Proof. Since n is prime, and we have $a \neq b$, we get that $a - b \not\equiv 0 \bmod n$, so σ^{b-a} is an n-cycle. Notice that in general we have $\sigma^k(x) = x + k$, so specifically, $\sigma^{b-a}(a) = a + b - a = b$. Thus σ is an n-cycle of the form $(a\ b \dots)$. Now we relabel elements of $\{1, 2, \dots n\}$ so that $\sigma = (1\ 2 \dots n)$. In particular, τ becomes $(1\ 2)$ in this new relabeling. So $\langle \sigma, \tau \rangle = \langle (1\ 2), (1\ 2 \dots) \rangle$. These two generate S_n by part (c), so σ, τ generate S_n. □