Homework 2
Algebra

Joshua Ruiter

April 7, 2018

Lemma 0.1 (for Exercise 1a). *Let G be a finite group. Then G has a maximal proper normal subgroup.*

Proof. Since G is finite, its power set is finite, so the collection of normal subgroups is finite. In particular, the subset of $\mathbb{N}$ given by

$$\{|H| : H \triangleleft G, H \neq G\}$$

is finite, so it has a maximum, call it m. Then there exists a normal subgroup H so that $|H| = m$. We claim that H is a maximal proper normal subgroup. Let K be a proper normal subgroup of G such that $H \subset K$, so $m = |H| \leq |K|$. Then by maximality of m, we have $|K| = m$. Thus K does not contain H properly, so H is a maximal normal subgroup. □

Lemma 0.2 (just for fun). *Every group has a maximal proper normal subgroup.*

Proof. The set of proper normal subgroups of G is partial ordered by $\subset$, and every totally ordered subset has an upper bound, namely G. Then by Zorn's Lemma, this set has a maximal element. □

Lemma 0.3 (for Exercise 1a). *Let $f : G \to G'$ be a group homomorphism and H a subgroup of G. Then $f(H)$ is a subgroup of G'.*

Proof. Let e, e' be the identites for G, G' respectively. Suppose $x', y' \in f(H)$. Then there exist $x, y \in H$ such that $f(x) = x', f(y) = y'$, so $xy \in H$ so $f(xy) = f(x)f(y) = x'y' \in f(H)$. Thus $f(H)$ is closed. We know that $f(e) = e'$, so $e' \in f(H)$. If $x' \in f(H)$, then there exists $x \in H$ so that $f(x) = x'$, so $x^{-1} \in H$, so $f(x^{-1}) = f(x)^{-1} \in f(H)$, so $f(H)$ is closed under inverses. Associativity in $f(H)$ follows from associativity in G'. □

Lemma 0.4 (for Exercise 1a). *Let $f : G \to G'$ be a surjective group homomorphism and N a normal subgroup of G. Then $f(N)$ is a normal subgroup of G'.*

Proof. We know that $f(N)$ is a subgroup by the above. Let $x' \in G'$. Then since f is surjective, there exists $x \in G$ such that $f(x) = x'$. Then we have

$$x'f(N) = f(x)f(N) = f(xN) = f(Nx) = f(N)f(x) = f(N)x'$$

so $f(N)$ is normal. □

Lemma 0.5 (for Exercise 1a). *Let G be a group and H a normal subgroup. Let $\pi : G \to G/H$ be the projection $g \mapsto gH$. If N is a proper normal subgroup of G such that $H \subset N$, then $\pi(N)$ is a proper normal subgroup of G/H.*

Proof. Let N be a proper normal subgroup of G with $H \subset N$. Since π is surjective, we know that $\pi(N)$ is a normal subgroup of G/H, so we just need to show that it is proper.

Suppose that $\pi(N) = G/H$. Then N contains an element from each coset of H, that is, for a coset aH we have $b \in N$ such that $bH = aH$. Then N contains bH, because $H \subset N$. Thus N contains all cosets of H, so N contains G, so $N = G$. This contradicts the assumption that N is a proper subgroup of G, so we must conclude that $\pi(N) \neq G/H$. □

Lemma 0.6 (for Exercise 1a). *Let G be a group and H a normal subgroup. Then G/H is simple if and only if H is maximal.*

Proof. Assume that H is maximal. Suppose G/H is not simple, that is, there exists a proper, nontrivial normal subgroup $K \triangleleft G/H$. Let $\pi : G \to G/H$ be the projection $g \mapsto gH$. Then since π is surjective, $\pi^{-1}(K)$ is a normal subgroup of G containing H. Since K is nontrivial, it contains a non-identity element kH where $k \notin H$. Then $k \in \pi^{-1}(K)$ but $k \notin H$, so H is a proper subset of $\pi^{-1}(K)$. This contradicts the fact that H is maximal, so we conclude that G/H is simple.

Now suppose that G/H is simple. Suppose that H is not maximal, that is, there is a proper normal subgroup N with $H \subset N$. Then $\pi(N)$ is a proper normal subgroup of G/H by Lemma 0.5, which contradicts G/H being simple. Thus H is maximal. □

Proposition 0.7 (Exercise 1a). *Every finite group G has a composition series, that is, a normal tower ending in the trivial group such that every quotient of adjacent groups $G_i = G_{i+1}$ is simple.*

Proof. If G is simple, then

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

is a normal tower with simple quotients. If G is not simple, then let G_1 be a maximal normal proper subgroup. If G_1 is simple, then

$$G \supset G_1 \supset \{e\}$$

is a normal tower with simple quotients. (G/G_1 is simple because G_1 is maximal.) Continuing in this manner, if G_i is not simple, we find a proper maximal normal subgroup G_{i+1}. We get normal tower with simple quotients, with $|G_{i+1}| \leq |G_i|$.

$$G \supset G_1 \supset G_2 \supset \ldots \supset G_k \supset \ldots \supset \{e\}$$

If at any point G_k is simple, we have a composition series

$$G \supset G_1 \supset \ldots \supset G_k \supset \{e\}$$

Since the order decreases at each step, after at most $|G|$ steps, we reach a subgroup G_n with order 1. Thus

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

is a composition series for G. □

Proposition 0.8 (Exercise 1a)**.** *Not every infinite group has a composition series.*

Proof. We claim that the abelian group $(\mathbb{Z}, +)$ has no composition series. Note that every subgroup is cyclic, and every subgroup except $\{0\}$ is $n\mathbb{Z}$ for some $n \in \mathbb{N}$. Suppose there is a normal tower

$$\mathbb{Z} = G \supset G_1 \supset G_2 \supset \ldots \supset G_{n-1} \supset G_n = \{0\}$$

where each quotient G_i/G_{i+1} is simple. Then $G_{n-1}/G_n = G_{n-1}$ is simple. But G_{n-1} contains $\{0\}$ as a proper subgroup, so it contains some $k \in \mathbb{Z}$, so $\langle k \rangle$ is a subgroup of G_{n-1}. If it is a proper subgroup, then G_{n-1} is not simple and we already obtain a contradiction. If $\langle k \rangle = G_{n-1}$, then we have $\langle 2k \rangle \subset G_{n-1}$ as a proper subgroup. Thus G_{n-1} is not simple, so no such tower exists. □

Lemma 0.9 (for Exercise 1b)**.** *Let G be a group with normal subgroup H such that G/H is abelian. Then $[G, G] \subset H$.*

Proof. We need to show that for $a, b \in G$, the commutator $aba^{-1}b^{-1} \in H$. Let $a, b \in G$. Since G/H is abelian,

$$abH = aHbH = bHaH = baH \implies ab(ba)^{-1} = aba^{-1}b^{-1} \in H$$

□

Lemma 0.10 (for Exercise 1b)**.** *Let G be group and H be a subgroup. Then $[H, H] \subset [G, G]$.*

Proof. $[G, G]$ is the subgroup generated by commutators $aba^{-1}b^{-1}$ with $a, b \in G$. H is the subgroup generated by commutators $cdc^{-1}d^{-1}$ with $c, d \in H$. Clearly, every commutator for H is a commutator for G, so the generating set for $[H, H]$ is a subset of the generating set for $[G, G]$. Thus $[H, H] \subset [G, G]$. □

Proposition 0.11 (Exercise 1b)**.** *Let G be a group and $G^{(1)} = [G, G]$ be the commutator group. Set $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Then G is solvable if and only if $G^{(n)} = \{e\}$ for some n.*

Proof. Suppose that $G^{(n)} = \{e\}$ for some n. By Exercise 3 from the last homework, $[G, G]$ is normal in G, and $G/[G, G]$ is abelian, so we have an abelian normal tower

$$G \supset G^{(1)} \supset G^{(2)} \supset \ldots \supset G^{(n)} = \{e\}$$

Hence G is solvable. Now suppose that G is solvable, that is, there is a normal abelian tower

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$$

For each i, G_{i+1} is a normal in G_i with G_i/G_{i+1} abelian, so by Lemma 0.9, $[G_i, G_i] \subset G_{i+1}$. Also, $G^{(1)} = [G, G] \subset G_1$. Now we induct on i, assuming that $G^{(k)} \subset G_k$ for $k = 1, \ldots i$. Then

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [G_i, G_i] \subset G_{i+1}$$

This completes the induction, so $G^{(i)} \subset G_i$ for all i. In particular, $G^{(n)} \subset G_n = \{e\}$ so $G^{(n)} = \{e\}$. □

Proposition 0.12 (Exercise 2)**.** *Let G be a p-group and N be a normal subgroup of order p. Then $N \subset Z(G)$.*

Proof. Let G act on N by conjugation. (This action is well-defined because N is normal.) Since G is a p-group and p divides $|N|$, the number of fixed points of this action is congruent to 0 mod p (by Lemma 6.3c in Lang). Since N is a subgroup, it contains e, and e is a fixed point of this action. Hence there are at least p fixed points of this action ($geg^{-1} = gg^{-1} = e$). But $|N| = p$ so all of N is fixed by conjugation from G. Hence for $x \in N, g \in G$ we have $gxg^{-1} = x \implies gx = xg$. Thus $N \subset Z(G)$. □

Proposition 0.13 (Exercise 12a)**.** *Let G be a group and N, H subgroups with N normal. Let $\psi : G \to \mathrm{Aut}(G)$ be $x \mapsto \psi_x$ where $\psi_x : G \to G$ is given by $g \mapsto gxg^{-1}$. Then ψ induces a homomorphism $f : H \to \mathrm{Aut}(N)$ given by $h \mapsto \psi_h|_N$.*

Proof. First we need to show that $\psi_h|_N$ is an automorphism of N. For $x \in N$, $\psi_h|_N(x) = hxh^{-1} \in N$ since N is normal, so we confirm that $\psi_h|_N$ does map into N. It is a homomorphism because for $x, y \in N$, we have

$$\psi_h|_N(xy) = hxyh^{-1} = hxh^{-1}hxh^{-1} = \psi_h|_N(x)\psi_h|_N(y)$$

Now we need to show that f is a homomorphism. Let $g, h \in H, x, y \in N$. Then

$$\begin{aligned} f(gh)(x) &= \psi_{gh}|_N(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1} \\ &= g\psi_h|_N(x)g^{-1} = \psi_g|_N \circ \psi_h|_N(x) = f(g) \circ f(h)(x) \end{aligned}$$

Thus $f(gh) = f(g) \circ f(h)$, so f is a homomorphism. □

Proposition 0.14 (Exercise 12b)**.** *Let G be a group with H, N subgroups and N normal, such that $H \cap N = \{e\}$. The map $\phi : H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection. Furthermore, ϕ is an isomorphism if and only if $f : H \to \mathrm{Aut}(G)$ given by $x \mapsto \psi_x|_N$ is trivial, that is, $f(x) = \mathrm{Id}_N$ for $x \in H$.*

Proof. We show that ϕ is surjective. If $xy \in HN$, then $(x, y) \in H \times N$ so $\phi(x, y) = xy$.

Now we show that ϕ is injective. Suppose that $x, w \in H, y, z \in N$ such that $\phi(x, y) = \phi(w, z)$, that is, $xy = wz$. Then $w^{-1}x = zy^{-1}$. Since $w^{-1}x \in H$ and $zy^{-1} \in K$ and $H \cap K = \{e\}$, we get $w^{-1}x = zy^{-1} = e$, so $w = x$ and $y = z$. Hence $(x, y) = (w, z)$ so ϕ is injective.

Now we show the last claim. Suppose that f is trivial, that is, $f(x) = \mathrm{Id}_N$ for $x \in H$. Then $\psi_x|_N = \mathrm{Id}_N$, so for $y \in N$, we have $xyx^{-1} = y \implies xy = yx$. Then for $x, w \in H, y, z \in H$, we have

$$\phi((x, y)(w, z)) = \phi(xw, yz) = xwyz = xywz = \phi(x, y)\phi(w, z)$$

thus ϕ is a bijective homomorphism, so it is an isomorphism.

Now suppose that ϕ is an isomorphism. Then for $x, w \in H, y, z \in N$ we have

$$xwyz = \phi(xw, yz) = \phi((x, y)(w, z)) = \phi(x, y)\phi(w, z) = xywz$$

thsun $yw = wy$ for all $w \in H, y \in N$. Thus

$$f(w)(y) = \psi_w|_N(y) = wyw^{-1} = yww^{-1} = y$$

so $f(w) = \mathrm{Id}_N$ for $w \in H$. □

Proposition 0.15 (Exercise 12c)**.** *Let N, H be groups and $\psi : H \to \text{Aut}(N)$ be a homomorphism. Let $G = \{(x, h) : x \in N, h \in H\}$ and define a binary operation on G by*

$$(x, f)(y, h) = (x\psi_f y, fh)$$

where we use the notation ψ_f to mean $\psi(f)$. Then G is a group under this operation. Furthermore, if we identify N with the set of elements (x, e_H) and H with the elements (e_N, h) then G is a semidirect product of N and H.

Proof. Let e_H, e_N be the respective identities of H, N. Then for $x \in N, h \in H$,

$$\begin{aligned}(e_N, e_H)(x, h) &= (e_N\psi_{e_N}x, e_H h) = (x, h)\\ (x, h)(e_N, e_H) &= (x\psi_h e_N, he_H) = (xe_N, h) = (x, h)\end{aligned}$$

so (e_H, e_N) is an identity for G. Closure is immediate from the definition, as $x\psi_f y \in N$. G is closed under inverses, as (x, h) has the inverse $(\psi_{h^{-1}}x^{-1}, h^{-1})$.

$$(x, h)(\psi_{h^{-1}}x^{-1}, h^{-1}) = (x\psi_h\psi_{h^{-1}}x^{-1}, hh^{-1}) = (xx^{-1}, hh^{-1}) = (e_N, e_H)$$

Finally, we need to show that associativity holds. Let $(x, f), (y, g), (z, h) \in G$.

$$\begin{aligned}(x, f) \cdot [(y, g) \cdot (z, h)] &= (x, f) \cdot (y(\psi_g z), gh)\\ &= (x\psi_f(y(\psi_g z)), fgh)\\ &= (x(\psi_f y)\psi_f(\psi_g z)), fgh)\\ &= (x(\psi_f y)(\psi_{fg} z), fgh)\\ &= (x(\psi_f y), fg) \cdot (z, h)\\ &= [(x, f) \cdot (y, g)] \cdot (z, h)\end{aligned}$$

So we have associativity. Thus G is a group. Now we identify N with $\{(x, e_H) : x \in N\} \subset G$ and H with $\{(e_N, h) : h \in H\} \subset G$. we can see that $H \cap N = \{(e_N, e_H)\}$ and $G = NH$, as $(x, h) \in G$ can be written as

$$(x, e_H)(e_N, h) = (x\psi(e_H)e_N, e_H h) = (x, h)$$

Thus G is the semidirect product of N and H. □

Proposition 0.16 (Exercise 14a)**.** *Let G be a finite group and let N be a normal subgroup such that N and G/N have relatively prime orders. Let H be a subgroup of G with the same order as G/N. Then $G = HN$.*

Proof. First, we claim that $H \cap N = \{e\}$. Suppose that $x \neq e$ and $x \in H \cap N$. Then $\langle x \rangle \subset H \cap N$, so $|x|$ divides $|H|$ and $|N|$. Since $x \neq e$ we know that $|x| \geq 2$, so this is a contradiction, since $|H|$ and $|N|$ are relatively prime. Thus the claim is proved.

By the second isomorphism theorem, HN is a subgroup of G, and

$$(HN)/N \cong H/(H \cap N) \cong H/\{e\} \cong H$$

Then by Lagrange's Theorem we have

$$|HN|/|N| = |H| \implies |HN| = |H||N| = |G/N||N| = |G|$$

Thus HN is a subgroup of G with the same order as G, so $HN = G$. □

Proposition 0.17 (Exercise 14b). *Let G be a finite group and let N be a normal subgroup so that N and G/N have relatively prime orders. Let $\phi : G \to G$ be an automorphism. Then $\phi(N) = N$.*

Proof. Suppose that $\phi(N) \neq N$. Then there exists $x \in N$ such that $\phi(x) \notin N$. We will reach a contradiction by showing that $|\phi(x)N|$ divides both $|N|$ and $|G/N|$.

Since $\phi(N)$ is a subgroup, $x \neq e$. We know that $|x| \neq 1$ and $|x|$ divides $|N|$, as $\langle x \rangle$ is a subgroup of N. Since $\phi(x) \notin N$, the coset $\phi(x)N$ is not equal to N, so $|\phi(x)N| \neq 1$. (Note: $|\phi(x)N|$ is the order of the coset $\phi(x)N$ in G/N.) Using the fact that ϕ is a homomorphism,

$$(\phi(x)N)^{|x|} = \phi(x)^{|x|}N = \phi(x^{|x|})N = \phi(e)N = eN = N$$

This calculation says that $|\phi(x)N|$ divides $|x|$, so it divides $|N|$. Since $\langle \phi(x)N \rangle$ is a cyclic subgroup of G/N, its order also divides $|G/N|$. Thus $|\phi(x)N|$ divides $|N|$ and $|G/N|$, which is a contradiction since these orders are relatively prime by hypothesis. So we reject our assumption and conclude that $\phi(N) = N$. $\square$

Note on notation: For a group G acting on a set S, we use the notation G_s for the stabilizer (isotropy) subgroup of G and $G.s$ for the orbit of s.

Lemma 0.18 (for Exercise 15). *Let G be a group acting on a set S. Then for $g \in G, a \in S$,*

$$gG_ag^{-1} = G_{ga}$$

Consequently, if $a, b \in S$ are in the same orbit, their isotropy groups are conjugate. Also, all subgroups conjugate to an isotropy group are isotropy groups.

Proof. First we show that $gG_ag^{-1} = G_{ga}$.

$$x \in gG_ag^{-1} \iff g^{-1}xg \in G_a \iff g^{-1}xga = a \iff xga = ga \iff x \in G_{ga}$$

If $a, b \in S$ are in the same orbit, then $b = ga$ for some $g \in G$. Then by the above, $G_b = G_{ga} = gG_ag^{-1}$ so G_b and G_a are conjugate. Finally, if H is conjugate to G_a, then by the above, $H = G_{ga}$ for some $g \in G$ so all conjugate subgroups to G_a are isotropy groups. $\square$

Proposition 0.19 (Exercise 15). *Let G be a finite group acting on a finite set S with $|S| \geq 2$, such that there is only one orbit. Then there exists $x \in G$ which has no fixed point ($xa \neq a$ for all $a \in S$).*

Proof. Let $a \in S$. The orbit of a is all of S, so the order of G_a is $|G|/|S|$. This is strictly less than G, as $|S| \geq 2$. Thus G_a is a proper subgroup of G. By the previous lemma, the conjugates of G_a are all isotropy subgroups. Then by exercise 16, the union of all isotropy subgroups is not equal to G. Hence there exists $x \in G$ such that $x \notin G_a$ for any $a \in S$, that is, $xa \neq a$ for all $a \in S$. $\square$

Proposition 0.20 (Exercise 16). *Let H be a proper subgroup of a finite group G. Then G is not the union of all the conjugates of H.*

Proof. We know that $N_G(H)$, the normalizer of H in G contains H, and $N_G(H)$ is a subgroup, so $[G : N_G(H)] \leq [G : H]$. Let K_H be the set of conjugate subgroups to H, that is,

$$K_H = \{gHg^{-1} : g \in G\}$$

We define a group action of G on K_H by conjugation, that is, $x \cdot (gHg^{-1}) = xgHg^{-1}x^{-1} = xgH(xg)^{-1}$. The stabilizer of H under this action is $N_G(H)$. By Proposition 5.2 from Lang, $|K_H| = [G : N_G(H)]$.

Each conjugate of H is isomorphic to H, so it has the same size as H, and it also contains the identity element. So the maximum number of non-overlapping elements in each conjugate subgroup to H is $|H| - 1$. As we showed, there are $|K_H| \leq [G : H]$ such subgroups.

$$\begin{aligned}
\#\left(\bigcup_{g \in G} gHg^{-1}\right) &\leq (|H| - 1)[G : N_G(H)] + 1 \\
&\leq (|H| - 1)[G : H] + 1 \\
&= |H|[G : H] - [G : H] + 1 \\
&= |G| - [G : H] + 1
\end{aligned}$$

(The $+1$ accounts for the identity.) Because H is a proper subgroup, $[G : H] \geq 2$. Thus this union has at most $|G| - 1$ elements, so it is not all of G. □

Proposition 0.21 (Exercise 19a)**.** *Let G be a finite group acting on a finite set S. Then for $s \in S$,*

$$\sum_{t \in G.s} \frac{1}{|G.t|} = 1$$

Proof. As $t \in G.s$, we have $G.t = G.s$. Thus $|G.t| = |G.s|$ so

$$\sum_{t \in G.s} \frac{1}{|G.t|} = \sum_{t \in G.s} \frac{1}{|G.s|} = |G.s| \frac{1}{|G.s|} = 1$$

□

Proposition 0.22 (Exercise 19b)**.** *Let G be a finite group acting on a finite set S. For each $x \in G$ define $f(x)$ to be the number of elements $s \in S$ such that $xs = s$. Then the number of orbits of G in S is equal to*

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

Proof. First, we note that $\sum_{x \in G} f(x)$ is equal to the number of ordered pairs $(x, s) \in G \times S$ such that $xs = s$. Similarly, $\sum_{s \in S} |G_s|$ also counts the number of ordered pairs (x, s) where $xs = s$, so these two sums are equal.

$$\sum_{x \in G} f(x) = \sum_{s \in S} |G_s|$$

By the Orbit-Stabilizer Theorem (Proposition 5.1 in Lang), $|G_s| = |G|/|G.s|$ so

$$\frac{1}{|G|}\sum_{x\in G} f(x) = \frac{1}{|G|}\sum_{s\in S} |G_s| = \frac{1}{|G|}\sum_{s\in S}\frac{|G|}{|G.s|} = \sum_{s\in S}\frac{1}{|G.s|}$$

We can write S as the disjoint union of the orbits,

$$S = \bigsqcup_{t\in S'} G.t$$

where S' is a set consisting of one representative from each orbit. Now we can rewrite our final sum as

$$\sum_{s\in S}\frac{1}{|G.s|} = \sum_{G.t\subset S}\sum_{s\in G.t}\frac{1}{|G.s|} = \sum_{G.t\subset S} 1$$

So we have

$$\frac{1}{|G|}\sum_{x\in G} f(x) = \sum_{G.t\subset S} 1$$

The sum on the right is exactly the number of orbits of G in S, so this is the equality we wanted to show. □