**Name: Adam Frank** **October 16, 2020**

# Math 637: Homework Chapter 3

1. (3.1.1)
Let $\varphi : G \to H$ be a homomorphism and let $E$ be a subgroup of $H$. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker \varphi \trianglelefteq G$.

*Proof.* Let $a, b \in \varphi^{-1}(E)$. Then $\varphi(ab^{-1}) = \varphi(a)(\varphi(b))^{-1}$. Since $\varphi(a), \varphi(b) \in E$ and $E$ is a subgroup, then $\varphi(a)(\varphi(b))^{-1} \in E$. Hence $\varphi^{-1}(E) \leq G$.

Suppose $E \trianglelefteq H$ and let $g \in G$. Let $x \in \varphi^{-1}(E)$ so that $\varphi(x) \in E$. We will see that $gxg^{-1} \in \varphi^{-1}(E)$ which is the same as $\varphi(gxg^{-1}) \in E$. From this, by Theorem 6 part (5) of chapter 3.1, we will have that $\varphi(E) \trianglelefteq G$. Note that $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)(\varphi(g))^{-1}$ is $\varphi(x)$ conjugate with $\varphi(g)$. By $E \trianglelefteq H$, we have $\varphi(g)\varphi(x)(\varphi(g))^{-1} = \varphi(gxg^{-1}) \in E$.

To show that $\ker \varphi \trianglelefteq G$ set $E = \{\mathbb{1}\}$. This is always normal in any group since $g\{\mathbb{1}\}g^{-1} = \{gg^1\} = \{\mathbb{1}\}$. But then $\ker \varphi = \varphi^{-1}(E)$ in this case, so the above entails that this is normal in $G$. □

2. (3.1.3)
Let $A$ be an abelian group and $B \leq A$. Prove that $A/B$ is abelian. Give an example of a non-abelian group $G$ containing a proper normal subgroup $N$ such that $G/N$ is abelian.

*Proof.* First we show that $A/B$ is a group. As noted in the examples after the definition of the natural projection, any abelian group is normal. From the theorem that all normal subgroups are the kernel of some homomorphism, we then know that $B = \ker \pi$ for some homomorphism $\pi$. Now from the theorem that the quotient group is defined for kernels of homomorphisms, we have that $A/B$ is a group.

Now let $x, y \in A$ so that $xB, yB \in A/B$. Then

$$(xB)(yB) = (xy)B = (yx)B = (yB)(xB)$$

The first and last equality come from the definition of the quotient group operation. The middle equality is by the abelianness of $A$.

Here is an example of a non-abelian group with a proper normal subgroup such that the quotient is abelian: Set $A = D_4$ and $B = \langle r \rangle$, which is to say that $B$ is the group of rotations. Then to see that $B \trianglelefteq D_4$ observe that for any $i = 0, 1, 2, 3$ we have $r^i B r^{-i} = B$ just because rotations commute with each other. If $r^i s$ is any reflection, and $r^j \in B$ then we'll show that $(r^i s)r^j(r^i s)^{-1} \in B$, which as we've noted earlier, suffices to show that $B \trianglelefteq A$.

$$\begin{aligned}(r^i s)r^j(r^i s)^{-1} &= r^i s r^j s r^{-i} \\ &= r^i r^{-j} s s r^{-i} \\ &= r^{i-j-i} = r^{-j} \in B\end{aligned}$$

Finally, to see that $A/B$ is abelian it is enough to show that it has order 2. Since

$$sB = s\{\mathbb{1}, r, r^2, r^3\} = \{s, sr, sr^2, sr^3\}$$

Since there can be no other cosests, the only two elements of $A/B$ are $B$ and $sB$. Since trivially any group of order 2 is abelian, $A/B$ is abelian.

□

3. (3.1.11(a))
Let $F$ be a field and $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in F, ac \neq 0 \right\} \leq GL_2(F)$.

(a) Prove that the map $\varphi : \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto a$ is a surjective homomorphism from $G$ onto $F^\times$. Describe the fibers and kernel of $\varphi$.

*Proof.* First that it's a homomorphism:

$$\varphi\left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right] = \varphi\begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix}$$

$$= ax$$

$$= \left[\varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right]\left[\varphi\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right]$$

Next we see that it's surjective. If $a \in F$ then $\varphi\begin{pmatrix} a & 0 \\ 0 & \mathbb{1} \end{pmatrix} = a$. Note that $\mathbb{1} \in F$ because $F$ is a field. □

4. (3.1.22(a))
Prove that if $H$ and $K$ are normal subgroups of a group $G$ then their intersection $H \cap K$ is also a normal subgroup of $G$.

*Proof.* If $g \in G$ then it suffices to show that $g(H \cap K)g^{-1} \subseteq H \cap K$. So let $gxg^{-1} \in g(H \cap K)g^{-1}$ where $x \in H \cap K$. Because $H$ is normal in $G$ we have $gxg^{-1} \in H$, and because $K$ is normal in $G$ we have $gxg^{-1} \in K$. Hence $gxg^{-1} \in H \cap K$. □

5. (3.1.42)
Assume both $H$ and $K$ are normal subgroups of $G$ with $H \cap K = \mathbb{1}$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$.

*Proof.* We first prove $x^{-1}y^{-1}xy \in H$. We already know $x \in H$ therefore $x^{-1} \in H$. Because $H \trianglelefteq G$ then $y^{-1}x(y^{-1})^{-1} \in H$ since this is conjugation of $x$ by $y^{-1}$. Then $x^{-1}y^{-1}xy \in H$.

Next we show $x^{-1}y^{-1}xy \in K$. We already know $y \in K$. Because $K \trianglelefteq G$ then $x^{-1}y(x^{-1})^{-1} \in H$ since this is conjugation of $y$ by $x^{-1}$. Then $x^{-1}y^{-1}xy \in K$.

Hence $x^{-1}y^{-1}xy \in H \cap K$ and therefore $x^{-1}y^{-1}xy = \mathbb{1}$. Multiply by $yx$ and you have

$$xy = yx$$

as desired. □

6. (3.2.4)
Show that if $|G| = pq$ for some primes $p$ and $q$ (not necessarily distinct) then either $G$ is abelian or $Z(G) = 1$.

*Proof.* If $Z(G) \neq \mathbb{1}$ then the order $|Z(G)|$ can only be either $p$ or $q$ or $pq$. If the order is $pq$ then $Z(G) = G$ and so $G$ is abelian. So it suffices to show that the order cannot be either $p$ or $q$.

Without loss of generality, suppose for contradiction that the order of $Z(G)$ is $p$. That is to say $|Z(G)| = p$. Let $g \in G \setminus Z(G)$ so that $g$ does not commute with some element. As a preliminary remark note that no non-identity element of $\langle g \rangle$ is in $Z(G)$ either, since if $g^i$ commutes with every $x \in G$ then

$$g^i x = x g^i \Leftrightarrow$$

$$g x g^{i-1} = x g^i \Leftrightarrow$$

$$gx = xg$$

So $g$ commutes with every $x \in G$ contrary to assumption. Further, this implies that the order of the group generated by both sets, $|\langle Z(G), g \rangle|$ is $|Z(G)||g|$. This is because for every $z_1, z_2 \in Z(G)$ and $h_1, h_2 \in \langle g \rangle$, the elements $z_1 h_1 = z_2 h_2$ if and only if $z_2^{-1} z_1 = h_2 h_1^{-1} \in \langle g \rangle \cap Z(G)$. So in that case $z_1 = z_2$ and $h_1 = h_2$. Thus every $z \in Z(G), h \in \langle g \rangle$ corresponds to a unique $zh \in \langle Z(G), g \rangle$. The number of such choices is $|Z(G)||g|$.

Now the order of $g$ is $p$ or $q$ or $pq$. If the order is $pq$ then $G$ is cyclic, so abelian, so $|Z(G)| = pq$ contrary to assumption.

Suppose the order of $g$ is $q$. Thus $|\langle Z(G), g \rangle| = pq$. Hence $G = \langle Z(G), g \rangle$. Thus if we pick any $a, b \in G$ then by the observations above, $a$ must have the form $z_a h_a$ for some $z_a \in Z(G)$ and $h_a \in \langle g \rangle$. Likewise $b = z_b h_b$ for some $z_b \in Z(G)$ and $h_b \in \langle g \rangle$. Now $z_a$ and $z_b$ commute with everything in $G$ by definition. $h_a$ and $h_b$ commute with everything in $\langle g \rangle$ trivially. So

$$ab = z_a h_a z_b h_b = z_a z_b h_a h_b = z_a z_b h_b h_a = z_b h_b z_a h_a = ba$$

This shows that $G$ is abelian, contrary to the assumption that $|Z(G)| = p < pq$.

Finally suppose that $|g| \neq q$ so that $|g| = p$. Notice that these two facts entail $p \neq q$. Also $|\langle Z(G), g \rangle| = p^2$, so $p^2 | pq$, so $p | q$, which is impossible for distinct primes. □

7. (3.2.7)
Let $H \leq G$ and let $g \in G$. Prove that if the right coset $Hg$ equals some left coset of $H$ in $G$, then it equals the left coset $gH$ and that $g \in N_G(H)$.

*Proof.* Suppose $Hg = xH$ for some $x \in G$. Since $xH = gH$ is equivalent to $g^{-1}x \in H$, we make this our goal. First note that $x \in xH$ since $\mathbb{1} \in H$, and hence $x \in Hg$. So there exists some $h \in H$ such that $x = hg$ and we get $g^{-1}x = h \in H$ as desired.

From $Hg = gH$ we can infer $H = gHg^{-1}$ so that $g \in N_G(H)$ by definition. □

8. (3.2.12)
Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of $H$ in $G$ onto a right coset of $H$, and gives a bijection between the set of left cosets and the set of right cosets of $H$ in $G$ (hence the number of left cosets equals the number of right cosets).

*Proof.* Let $gH$ be any left coset and let $gh \in gH$ be any element. Then $gh \mapsto (gh)^{-1} = h^{-1}g^{-1}$. Since $h^{-1} \in H$ then $h^{-1}g^{-1} \in Hg^{-1}$. Thus the map sends every element of $gH$ to some element of $Hg^{-1}$.

To see that this map is onto, let $hg^{-1} \in Hg^{-1}$. Since $h^{-1} \in H$ then $gh^{-1} \in gH$ and the map sends this to $(gh^{-1})^{-1} = hg^{-1}$, as desired.

Now we use this to build a bijection between the set of left cosets, $G/H$, and the set of right cosets, $H\backslash G$. Namely, let $\varphi(gH) = Hg^{-1}$. We first need to see that this map is well-defined, then that it's a bijection. To see that it's well-defined suppose that $g_1H = g_2H$ and note that this is equivalent to $g_2^{-1}g_1 \in H$. Therefore we have $(g_2^{-1}g_1)^{-1} \in H$, which is the same as $g_1^{-1}g_2 \in H$. But this entails $Hg_1^{-1}g_2 = H$ so that $Hg_1^{-1} = Hg_2^{-1} = \varphi(g_1H) = \varphi(g_2H)$, and this shows $\varphi$ is well-defined.

Next we show that $\varphi$ is injective. If

$$\varphi(g_1H) = \varphi(g_2H) = Hg_1^{-1} = Hg_2^{-1}$$

then $g_2^{-1}g_1 \in H$ so $(g_2^{-1}g_1)^{-1} = g_1^{-1}g_2 \in H$. So $g_1H = g_2H$ and thus $\varphi$ is injective. To see that it's surjective, note that for any $Hg$ we have $\varphi(g^{-1}H) = Hg$.

Since this is a bijection between $G/H$ and $H\backslash G$ then the number of right cosets is the number of left cosets. □

9. (3.2.16)
Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's Little Theorem: if $p$ is a prime then $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

*Proof.* First note that the result holds trivially if $a \equiv 0 \mod p$. So for the rest of the proof assume $a \not\equiv 0 \mod p$.

Now we show that $a^{p-1} \equiv 1 \mod p$. Since $a \not\equiv 0 \mod p$ then $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Moreover $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$, and any element to the order of the group is the identity. Hence $\overline{a}^{p-1} = \overline{1}$ and so $a^{p-1} \equiv 1 \mod p$. This of course implies the desired $a^p \equiv a \mod p$. □

10. (3.3.3)
Prove that if $H \trianglelefteq G$ and $|G : H| = p$ where $p$ is prime, then for all $K \leq G$ either

(i) $K \leq H$ or

(ii) $G = HK$ and $|K : K \cap H| = p$.

*Proof.* Since $H \trianglelefteq G$ then $HK$ is a subgroup by corollary 15. Also since $H \trianglelefteq G$ then $G/H$ is a group and has order $p$. If (i) does not hold then there is some $k \in K \smallsetminus H$ and therefore $H < HK$. Now due to the Fourth Isomorphism Theorem $HK/H \leq G/H$ and therefore $|HK/H|$ divides $p$ by Lagrange's Theorem. Since $|HK/H| \leq p$ then $|HK/H|$ must be either 1 or $p$. It cannot be 1 since that would entail $HK = H$ which entails $K \leq H$. Therefore $|HK/H| = p$ but then $HK/H = G/H$ so again by the Fourth Isomorphism Theorem (using $\leq$ in both directions) we have $G = HK$.

And since $|G : H| = p = |HK : H| = |K : K \cap H|$ then we have the second part immediately. □

11. (3.3.8)
Let $p$ be a prime and $G$ the group of $p$-power roots of 1 in $\mathbb{C}$. Prove that the map $z \mapsto z^p$ is a surjective homomorphism. Deduce that $G$ is isomorphic to a proper quotient of itself.

*Proof.* Let $a$ and $b$ be any $p$-power root of 1, that is to say, there is some $m, n \in \mathbb{N}$ such that $a^{p^m} = 1 = b^{p^n}$. First let's show the given map is a homomorphism. Call the mapping $\varphi$ so that

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$$

where the power distributes because complex numbers commute.

Next we show that it's surjective by finding a $p$-power root which maps to $a$. First we note that $(a^{1/p})^{p^{n+1}} = 1$ then this shows that $a^{1/p} \in G$. Then of course $\varphi(a^{1/p}) = a$.

Finally to deduce that $G$ is isomorphic to a proper quotient of itself, we appeal to the First Isomorphism Theorem. This guarantees that the image of the map is isomorphic to the $G/\ker\varphi$. Then

$$\mathrm{Im}\varphi = G \cong G/\ker\varphi$$

all that remains to show is that $\ker\varphi \neq \mathbb{1}$. But since $1 \mapsto 1$ and $e^{i2\pi/p} \mapsto 1$ then we are done. □

12. (3.3.9)
Let $p$ be a prime and let $G$ be a group of order $p^\alpha m$ where $p \nmid m$. Assume $P$ is a subgroup of $G$ of order $p^\alpha$ and $N$ is a normal subgroup of $G$ of order $p^b n$ where $p \nmid n$. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{\alpha - b}$.

*Proof.* Since $P \cap N \leq P$ we must have $|P \cap B|$ divides $p^\alpha$. Therefore $|P \cap N| = p^x$ for some non-negative integer $x$. Moreover since $P \cap N \leq N$ then $p^x | p^b n$. Since $p$ is prime and $p \nmid n$ then we have that $p^x | p^b$ and so $x \leq b$.

Now since $N \trianglelefteq G$ then $NP \leq G$ and therefore $|NP|$ divides $|G| = p^\alpha m$. But also $|NP| = |N||P|/|P \cap N| = p^{\alpha+b} n / p^x$ and hence $p^{\alpha+b-x} n$ divides $p^\alpha m$. In particular this implies that $p^{\alpha+b-x}$ divides $p^\alpha$. Hence $b - x \leq 0$, which is the same as $b \leq x$. Together with the inequality from earlier, we now have $b = x$, that is to say $|P \cap N| = p^b$.

Finally due to the Second Isomorphism Theorem $|PN/N| = |P|/|P \cap N| = p^\alpha / p^b = p^{\alpha - b}$. □

13. (3.4.1)
Show that every simple abelian group is isomorphic to $Z_p$ for some prime $p$.

*Proof.* Let $x \in G$ be any non-identity element and consider the subgroup it generates, $\langle x \rangle \leq G$. Since $G$ is abelian every subgroup is normal, so $G = \langle x \rangle$. Now if the order of $x$ is not prime, then there is a subgroup of $\langle x \rangle$ of order this divisor, and this subgroup would be normal. Since that cannot exist, the order of $x$ is some prime $p$. Then under the explicit bijection with $Z_p$ determined by $x \mapsto \mathbb{1}$ we see that these groups are isomorphic. □

14. (3.4.11)
Prove that if $H$ is a non-trivial normal subgroup of the solvable group $G$ then there is a non-trivial subgroup $A \leq H$ and further $A \trianglelefteq G$, and $A$ abelian.

*Proof.* Since there is a non-trivial normal subgroup, then in the chain of normal subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_s = G$$

we can construct the "solution series" for $H$:

$$1 = G_0 \cap H \trianglelefteq G_1 \cap H \trianglelefteq \cdots \trianglelefteq G_s \cap H$$

To see that this is a solution series for $H$, we first show that $G_i \cap H \trianglelefteq G_{i+1} \cap H$ for each $i = 0, \ldots, s-1$. First note that if $y \in G_{i+1} \cap H$ and $x \in G_i \cap H$ then $yxy^{-1} \in G_i$ because $G_i \trianglelefteq G_{i+1}$. Also $yxy^{-1} \in H$ because $H \trianglelefteq G$. So $yxy^{-1} \in G_i \cap H$ which shows that $G_i \cap H \trianglelefteq G_{i+1} \cap H$.

Next we see that $(G_{i+1} \cap H)/(G_i \cap H)$ is abelian. The Second Isomorphism Theorem guarantees that if subgroups satisfy $X \leq N_G(Y)$ then

$$XY/Y \cong X/(X \cap Y)$$

Here we can set $X = G_{i+1} \cap H$ and $Y = G_i$. Since $G_i \subseteq G_{i+1}$ then $X \cap Y = (G_{i+1} \cap H) \cap G_i = G_i \cap H$. From this we get the isomorphism

$$\frac{G_{i+1} \cap H}{G_i \cap H} \cong \frac{(G_{i+1} \cap H)(G_i \cap H)}{G_i} = \frac{G_{i+1}G_i \cap H}{G_i} = \frac{G_{i+1} \cap H}{G_i}$$

Now $(G_{i+1} \cap H)/G_i$ is a subgroup of $G_{i+1}/G_i$, and the latter is an abelian subgroup. Therefore $(G_{i+1} \cap H)/G_i$ is abelian, and as this is isomorphic to $\frac{G_{i+1} \cap H}{G_i \cap H}$ then this too is abelian, as desired.

Now that we know that the above is a solution series, we may take the least index $i$ such that $G_i \cap H$ is not the trivial group. We call this index $j$. This must exist since $G_s \cap H = H$ is assumed to be nontrivial. Since $G_{j-1} \cap H = \mathbb{1}$ by minimality, we are now guaranteed that $(G_j \cap H)/\mathbb{1}$ is abelian, which is trivially isomorphic to $G_j \cap H$. Moreover, $G_j \cap H \leq H$. All that remains is to confirm that $G_j \cap H \trianglelefteq G$.

For this part we proceed by induction. Since $G_j \trianglelefteq G_{j+1}$ and $H \trianglelefteq G_{j+1}$ because $H \trianglelefteq G$, then it follows that $G_j \cap H \trianglelefteq G_{j+1}$, which is our base-case. For the inductive case suppose that $G_j \cap H \trianglelefteq G_{j+k}$. If $x \in G_{j+k+1}$ and $y \in G_j \cap H$ then we have $xyx^{-1} \in G_{j+k} \cap H$. □

15. (3.5.12)
Prove that $A_n$ contains a subgroup isomorphic to $S_{n-2}$ for each $n \geq 3$.

*Proof.* We build an injective homomorphism $\varphi : S_{n-2} \to A_n$. For any even permutation $\sigma \in S_n$ we assign $\varphi(\sigma) = \sigma$. That is to say, if $\sigma(i) = j$ in $S_{n-2}$, then $\varphi(\sigma)(i) = j$ in $A_n$ for each $i = 1, \ldots, n-2$ and $\varphi(\sigma)(n-1) = n-1$ and $\varphi(\sigma)(n) = n$. For any odd permutation $\sigma \in S_{n-2}$, we assign $\varphi(\sigma) = \sigma(n-1\ n)$. That is to say, for each $i = 0, \ldots, n-2$ we have $\varphi(\sigma)(i) = \sigma(i)$, and $\varphi(\sigma)(n-1) = n$ and $\varphi(\sigma)(n) = n-1$.

First let's see that this is a homomorphism. We proceed by cases. If $\sigma, \tau \in S_{n-2}$ are both even then

$$\varphi(\sigma\tau) = \sigma\tau = \varphi(\sigma)\varphi(\tau)$$

If one of $\sigma$ or $\tau$ are odd, without loss of generality suppose it's $\sigma$. Then since the product of an even and odd permutation is odd,

$$\varphi(\sigma\tau) = \sigma\tau(n-1\ n) = (\sigma(n-1\ n))\tau = \varphi(\sigma)\varphi(\tau)$$

where $(n-1\ n)$ commutes because it is disjoint from $\sigma, \tau \in S_{n-2}$. If both $\sigma, \tau$ are odd then their product is even and

$$\varphi(\sigma\tau) = \sigma\tau = \sigma(n-1\ n)(n-1\ n)\tau = \varphi(\sigma)\varphi(\tau)$$

So we now have that $\varphi$ is a homomorphism. To see that it's injective, suppose $\varphi(\sigma) = \varphi(\tau)$ and consider the case that $\varphi(\sigma)$ fixes $n-1$ and $n$. Then $\varphi(\sigma) = \sigma = \varphi(\tau) = \tau$. On the other hand suppose $\varphi(\sigma)$ transposes $n-1$ and $n$. Then $\varphi(\sigma) = \sigma(n-1\ n) = \varphi(\tau) = \tau(n-1\ n)$ and therefore $\sigma = \tau$. In all cases $\varphi(\sigma) = \varphi(\tau)$ entails $\sigma = \tau$ and so $\varphi$ is injective.

Then since $S_{n-2}$ is embedded in $A_n$, we have that the image of this embedding is a subgroup of $A_n$ which is isomorphic to $S_{n-2}$. □