Homework Assignment 5 Solutions

1. We begin by proving the fourth isomorphism theorem. Let $N \trianglelefteq G$ be a normal subgroup of a group G. Let $\pi : G \to G/N$ be the natural projection.

   (a) Let $H \leq G/N$. Show that the preimage $\pi^{-1}(H) = \{g \in G : \pi(g) \in H\}$ is a subgroup of G containing N.

   Proof. The preimage $\pi^{-1}(H) = \{g \in G : \pi(g) \in H\}$. If $a, b \in \pi^{-1}(H)$, then

   $$\pi(ab^{-1}) = \pi(a)\pi(b)^{-1} \in H,$$

   so that $ab^{-1} \in \pi^{-1}(H)$. Therefore by the subgroup criterion (HW4#1(a)), we see $\pi^{-1}(H) \leq G$. To see that it contains N, notice that for each $n \in N$ we have $\pi(n) = 1 \in H$, so $n \in \pi^{-1}(H)$. □

   (b) Let $H \leq G$. Show that its image $\pi(H)$ is a subgroup of G/N.

   Proof. Suppose $x, y \in \pi(H)$, so that $x = \pi(a)$ and $y = \pi(b)$ for $a, b \in H$. Therefore $ab^{-1} \in H$ so that

   $$xy^{-1} = \pi(a)\pi(b)^{-1} = \pi(ab^{-1}) \in \pi(H).$$

   Thus by the subgroup criterion (HW4#1(a)) $\pi(H) \leq G/H$. □

   (c) These constructions do not give a bijection between subgroups of G and subgroups of G/N. Give an example showing why.

   Proof. This construction will always map all subgroups of N to the trivial subgroup $1 \leq G/N$. So for example, let $G = \mathbb{Z}$, $N = 2\mathbb{Z}$, and let $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the projection. If $H = 4\mathbb{Z} \leq N$, then $\pi(N) = \pi(H) = \{\overline{0}\}$, so that the identification $H \mapsto \pi(H)$ is not injective.

   A more general example is if $\{1\} \neq N \trianglelefteq G$, and $\pi : G \to G/N$ is the projection then $\pi(N) = \pi(\{1\}) = \{1N\}$, so injectivity fails again. In fact, as the following exercise shows, this is the only kind of thing that can go wrong. □

   (d) If we restrict our attention to certain subgroups of G we do get a bijection. Show that the constructions in parts (a) and (b) give a bijection:

   $$\left\{ \begin{array}{c} \text{Subgroups } H \leq G \\ \text{such that } N \leq H \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{Subgroups} \\ \overline{H} \leq G/N \end{array} \right\}$$

   Proof. Part (b) show that $H \mapsto \pi(H)$ from the left to the right is well defined, and part (a) shows that $\overline{H} \mapsto \pi^{-1}(\overline{H})$ is. We must show these are inverses to eachother.

   We first show that $\pi(\pi^{-1}(\overline{H})) = \overline{H}$. First notice that

   $$\pi(\pi^{-1}(\overline{H})) = \{\pi(h) : h \in \pi^{-1}(\overline{H})\} \subseteq \overline{H}.$$

To show the reverse incusion, fix some $\overline{h} \in \overline{H}$, there is some $h \in G$ such that $\pi(h) = \overline{h}$ (since the natural projection to the quotient is always surjective). But then certainly $h \in \pi^{-1}(H)$ so that $\overline{h} = \pi(h) \in \pi(\pi^{-1}(\overline{H}))$. This shows that $\overline{H} \subseteq \pi(\pi^{-1}(\overline{H}))$ and completes the proof that $\varphi \circ \psi$ is the identity.

We next show $\pi^{-1}(\pi(H)) = H$. First notice that

$$\begin{aligned} \pi^{-1}\pi(H) &= \{g \in G : \pi(g) \in \pi(H)\} \\ &= \{g \in G : \pi(g) = \pi(h) \text{ for some } h \in H.\} \\ &\supseteq H. \end{aligned}$$

To finish we must show that $\pi^{-1}(\pi(H)) \subseteq H$, so fix some $g \in G$ and suppose that $\pi(g) = \pi(h)$ for some $h \in H$. If we show $g \in H$ we win. Notice $\pi(hg^{-1}) = \pi(g)\pi(h)^{-1} = 1$, so that $gh^{-1} \in N$. Since we assumed $N \leq H$ we have $gh^{-1} \in H$. Multiplying on the right by h and we conclude $g \in H$. Thus $\pi^{-1}(\pi(H)) = H$ and we win. □

(e) This bijection satisfies certain properties. First let's establish some notation. Let $H, K \in G$ be two subgroups containing N, and denote the corresponding subgroups of G/N by $\overline{H}$ and $\overline{K}$. Prove the following properties.

i. $H \leq K$ if and only if $\overline{H} \leq \overline{K}$.

Proof. By HW4#1(c) we don't need to worry about subgroup criteria, just containment, so this just boils down to some set theory. For the forward direction, notice that if $H \leq K$ then it is immediate that $\pi(H) \leq \pi(K)$, (since π of an element in H is automatically π of the same element which is also in K). Conversely, if $\overline{H} \leq \overline{K}$, then $\pi^{-1}(\overline{H}) \leq \pi^{-1}(\overline{K})$, (arguing analogously that if π of some element lands in $\overline{H}$ it lands in $\overline{K}$). □

ii. $H \trianglelefteq K$ if and only if $\overline{H} \trianglelefteq \overline{K}$.

Proof. Observe that the restriction of π to H, $\pi : H \to \overline{H}$, is surjective with kernel N so that $\overline{H} \cong H/N$, and similarly for K. Therefore the forward direction is exactly the third isomorphism theorem, applied to $N, H \trianglelefteq K$ with $N \leq H$.

Conversely, suppose $\overline{H} \trianglelefteq \overline{K}$. One can consider the composition:

$$K \xrightarrow{\pi} \overline{K} \longrightarrow \overline{K}/\overline{H}.$$

This is a homomorphism whose kernel consists of elements $k \in K$ such that $\pi(k) \in \overline{H}$. But this is precisely $\pi^{-1}(\overline{H}) = H$. Thus H is the kernel of a homomorphism and therefore normal (by HW4#7(c)). □

iii. $\overline{H \cap K} = \overline{H} \cap \overline{K}$

Proof. We use that $\overline{H} \cap \overline{K}$ is the largest subgroup contained in both H and K. We know that $\overline{H \cap K}$ is contained in both $\overline{H}$ and $\overline{K}$ (by part (i) for example), so that it must be contained in their intersection. Suppose that $\overline{P} \leq \overline{H} \cap \overline{K}$. Then in particular $\overline{P} \leq \overline{H}$ and $\overline{P} \leq \overline{K}$, so that by part (i), $P \leq H$ and $P \leq K$, thus $P \leq H \cap K$. This shows (again by part (i)) that $\overline{P} \leq \overline{H \cap K}$, so that the latter is indeed the largest subgroup contained in both $\overline{H}$ and $\overline{K}$, and is therefore their intersection. □

iv. $\overline{\langle H, K\rangle} = \langle \overline{H}, \overline{K}\rangle$.

Proof. This proof is exactly dual to part (iii), replacing $\leq$ with $\geq$ at each step.

We use that $\langle \overline{H}, \overline{K}\rangle$ is the smallest subgroup containing both H and K. We know that $\overline{\langle H, K\rangle}$ contains in both $\overline{H}$ and $\overline{K}$ (by part (i) for example), so that it must contain the subgroup they generate. Suppose that $\overline{P} \geq \langle \overline{H}, \overline{K}\rangle$. Then in particular $\overline{P} \geq \overline{H}$ and $\overline{P} \geq \overline{K}$, so that by part (i), $P \geq H$ and $P \geq K$, thus $P \geq \langle H, K\rangle$. This shows (again by part (i)) that $\overline{P} \geq \overline{\langle H, K\rangle}$, so that the latter is indeed the smallest subgroup containing both $\overline{H}$ and $\overline{K}$, and is therefore the subgroup they generate. □

Hint. *You can do (iii) and (iv) directly, but if you want to be really slick use that the intersection of two subgroups is the largest subgroup contained in both, (and the dual notion for the subgroup generated by two subgroups). Notice that this means that being the intersection of two subgroups (or generated by two subgroups) is a condition on the lattice of G (or G/N). Then the result should easily follow from part (i).*

Now let's establish some properties of one more family of finite groups, diverging from D_{2n}, S_n and direct products of cyclic groups. As we start defining more exotic properties of groups we will need to expand our library of finite groups to exhibit some of these interesting properties. Let's finish by introducing finite matrix groups. We will need a definition.

Definition 1. *A field is a set F together with two commutative binary operations, $+$ and $\cdot$ (addition and multiplication), such that $(F, +)$ and $(F \backslash \{0\}, \cdot)$ are abelian groups, and such that the distributive law holds. That is, for all $a, b, c \in F$ we have:*

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

For any field we let $F^\times = F \setminus \{0\}$ be its mutliplicative group. A field F is called a finite field if $|F| < \infty$.

It turns out that vector space theory over F is pretty much identical to vector space theory over R. We can define the first matrix group we hope to study.

Definition 2. *Let F be a field. If M, N are matrices with entries in F, we can compute their product MN and the determinant $\det(M) \in F$ using the same formulas as if $F = \mathbb{R}$. Then the general linear group of degree n over F is,*

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries in } F \text{ and } \det(A) \neq 0\}.$$

You may use the following facts without proofs (since they are a standard result of linear algebra).

Proposition 1. *The set $GL_n(F)$ can be identified with the set of linear bijections $F^n \to F^n$, and matrix multiplication corresponds to composition of functions. In particular, $GL_n(F)$ is a group under matrix multiplication.*

Proposition 2. *If $A, B \in GL_n(F)$, then $\det(AB) = \det(A)\det(B)$. In particular, $\det : GL_n(F) \to F^\times$ is a group homomorphism.*

2. It turns out that we have seen examples of finite fields already.

(a) Let p be a prime number. Show that $\mathbb{Z}/p\mathbb{Z}$ with the operations $+$ and $\times$ is a field. This is the *finite field of order* p and will be denoted by $\mathbb{F}_p$.

Proof. We already have seen that $\mathbb{Z}/p\mathbb{Z}$ is an abelian group under addition. Furthermore, by the extended Euclidean algorithm we know that an integer has a multiplicative inverse mod p if and only if it is coprime to p, so that every element of $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ has a multiplicative inverse, making it an abelian group under multiplication. Finally, multiplication and addition are inherited from the same operations on $\mathbb{Z}$ which satisfy the distributive law. □

(b) Show that if n is not prime, $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Proof. By the extended Euclidean algorithm, $a \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$. Therefore, letting $a|n$ and $a \neq 1$, we have $a \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ without a multiplicative inverse, so that $\mathbb{Z}/n\mathbb{Z}$ cannot be a field. □

3. Now let's study $GL_2(\mathbb{F}_p)$.

(a) Prove that $|GL_2(\mathbb{F}_2)| = 6$.

Proof. We will do parts (a) and (b) together, listing all the elements to see that there are 6 of them. A general matrix looks like

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Notice first that a and b can't both be 0. In each case, we fix (a, b) and leverage the fact that (c, d) must not be a multiple of (a, b). There are 3 cases, each with two possibilities. First, $a = 1$ and $b = 0$.

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

The case wehre $a = 0$ and $b = 1$ is similar.

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad D = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Finally, we have the case $a = b = 1$.

$$E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Thus there are six elements. □

(b) Write all the elements of $GL_2(\mathbb{F}_2)$ and compute the order of each element.

Proof. $A = I$ is the identity element and therefore has order 1. One can compute directly that $B^2 = C^2 = E^2 = I$ are the identity as well, thus they have order 2. But notice that $D^2 = F$ and that F^2 is D. Nevertheless, we notice that $F = D^{-1}$ so that $DF = FD = I$ so that $D^3 = F^3 = I$ so that they have order 3. □

(c) Show that $GL_2(\mathbb{F}_2)$ is not abelian. (We will later see that it is isomorphic to S_3).

Proof. We can check directly that $BC = D$ and that $CB = F$.

This isn't part of the assignment, but one can directly check now that $\varphi : GL_2(\mathbb{F}_2) \to S_3$ given by the rule:

$$\begin{aligned} A &\mapsto (1) \\ B &\mapsto (12) \\ C &\mapsto (23) \\ D &\mapsto (123) \\ E &\mapsto (13) \\ F &\mapsto (132) \end{aligned}$$

is an isomorphism. You will give a better proof of this fact in HW6#3 where you show any nonabelian group of order 6 is isomorphic to S_3. □

(d) Generalizing part (a), show that if p is prime then

$$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.$$

Proof. Fix some:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We want to count how many choices of (a, b, c, d) we have. We will use the fact that $\det A \neq 0$ if and only if the (c, d) is not a multiple of (a, b). Let's notice that the total number should be the product of the choices for (a, b) with the choices for (c, d) having fixed (a, b). Let's begin by counting the number of choices for (a, b). They must be selected from $\mathbb{F}_p$, so that we have p choices each for a and p choices for b, giving p^2 total choices. Of course, they cannot both be 0, $p^2 - 1$ allowable ones. Now all we have to say is that (c, d) is not a multiple of (a, b). That is, there are p^2 choices for (c, d), but p of them are $(\lambda a, \lambda b)$ for all the different $\lambda \in \mathbb{F}_p$. In particular, there are $p^2 - p$ allowable choices. Thus the total is:

$$(p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p.$$

□

4. The general linear group has lots of interesting subgroups and quotients.

(a) Show that the constant diagonal matrices are a normal subgroup of $GL_n(F)$ isomorphic to $F^\times$.

Proof. Define a homomorphism $\varphi : F^\times \to GL_n(F)$ given by the rule:

$$\varphi(\lambda) = \lambda \cdot I = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda \end{pmatrix}$$

This map is certainly injective, and its image is precisely the constant diagonal matrices, so that the constant diagonal matrices are a subgroup isomorphic to $F^\times$. To see they are normal, notice:

$$M\varphi(\lambda)M^{-1} = M\lambda \cdot IM^{-1} = \lambda \cdot (MIM^{-1}) = \lambda \cdot I = \varphi(\lambda).$$

(In fact, we just showed that the constant diagonal matrices are contained in $Z(GL_n(F))$). □

We will often abuse notation and denote this by $F^\times \trianglelefteq GL_n(F)$. The quotient group $GL_n(F)/F^\times$ is called the *projective general linear group* and denoted $PGL_n(F)$.

(b) The *special linear group* $SL_n(F)$ is defined

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1.\}$$

Show that $SL_n(F)$ is a normal subgroup of $GL_n(F)$ and prove that

$$GL_n(F)/SL_n(F) \cong F^\times.$$

Proof. By Proposition 2 above, $\det : GL_n(F) \to F^\times$ is a homomorphism, and by definition $SL_n(F) = \ker(\det)$. This gives normality, and if det is surjective the desired isomorphism follows immediately from the first isomorphism theorem. Fix $\lambda \in F^\times$ and let A be the matrix

$$A = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then $\det(A) = \lambda$ proving surjectivity. □

(c) List all the elements of $SL_2(\mathbb{F}_2)$

Proof. This is a bit of a trick question. Indeed, in $\mathbb{F}_2$ the only element not equal to 0, is 1. In particular, if $\det(A) \neq 0$ then $\det(A) = 1$. Therefore $SL_n(\mathbb{F}_2) = GL_n(\mathbb{F}_2)$ so that the answer is the same as 4(b). □

(d) Compute $|SL_2(\mathbb{F}_p)|$ (*Hint*, between 3(d) and 4(b) you've already done all the work).

Proof. By part (b), and Lagrange's theorem we know that:

$$\frac{|GL_n(\mathbb{F}_p)|}{|SL_n(\mathbb{F}_p)|} = |GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p)| = |\mathbb{F}_p^\times| = p - 1.$$

Therefore using 3(d) we compute

$$|SL_n(\mathbb{F}_p)| = \frac{|GL_n(\mathbb{F}_p)|}{|\mathbb{F}_p^\times|} = \frac{p^4 - p^3 - p^2 + p}{p-1} = p^3 - p.$$

□

(e) Let I be the identity matrix. Show that $\{\pm I\} \leq SL_n(F)$ if and only if n is even.

Proof. Notice that $I \in SL_n(F)$ always. On the other hand, $\det(-I) = (-1)^n$, giving the result, which is 1 if and only if n is even, giving the result. □

(f) Use the second isomorphism theorem to construct an isomorphism:

$$PGL_2(\mathbb{C}) \cong SL_2(\mathbb{C})/\{\pm I\}.$$

(As a bonus, think about why this is not true for a general field. For example, it is false over $\mathbb{R}$, or over $\mathbb{F}_p$ for $p \neq 2$.)

Proof. For any field F one can consider the following diamond.

$$\begin{tikzcd}
& GL_2(F) \arrow[d, dash] & \\
& SL_2(F) \cdot F^\times \arrow[dl, dash] \arrow[dr, dash] & \\
SL_2(F) \arrow[dr, dash] & & F^\times \arrow[dl, dash] \\
& SL_2(F) \cap F^\times &
\end{tikzcd}$$

The second isomorphism theorem immediately tells us:

$$(SL_2(F) \cdot F^\times)/F^\times \cong SL_2(F)/(SL_2(F) \cap F^\times). \tag{1}$$

We next show that $SL_2(F) \cap F^\times = \{\pm I\}$. Given a constant diagonal matrix λI its determinant is λ^2, which is 1 if and only if $\lambda = \pm 1$. Plugging into Equation 1 gives

$$(SL_2(F) \cdot F^\times)/F^\times \cong SL_2(F)/\{\pm 1\}, \tag{2}$$

which is close to the desired result. In order to win, we must show that:

$$SL_2(F) \cdot F^\times = GL_2(F). \tag{3}$$

Equivalently, that every invertible matrix is a scaled multiple of a matrix with determinant 1. Whether or not this is true actually depends on the arithmetic of F, and in particular, whether or not F has all of its square roots. To see this, let's now specialize to $F = \mathbb{C}$. Observe that for $\lambda \in \mathbb{C}^\times$, we know $\det(\lambda A) = \lambda^2 \det A$. Fix $A \in GL_n(\mathbb{C})$, with $\det(A) = d$. Then $\lambda = 1/\sqrt{d} \in \mathbb{C}^\times$ (here we use that we are working with complex numbers so square roots exist), and therefore:

$$\det(\lambda A) = \lambda^2 \det A = \left(\frac{1}{\sqrt{d}}\right)^2 d = 1.$$

Therefore $\lambda A \in SL_2(\mathbb{C})$ and so $A = (\lambda A)(\lambda^{-1} I) \in SL_2(\mathbb{C}) \cdot \mathbb{C}^\times$. This shows that $GL_2(\mathbb{C}) \subseteq SL_2(\mathbb{C}) \cdot \mathbb{C}^\times$ and thus they are equal. Plugging into Equation 2 gives:

$$PGL_2(\mathbb{C}) = GL_2(\mathbb{C})/\mathbb{C}^\times = (SL_2(\mathbb{C}) \cdot \mathbb{C}^\times)/\mathbb{C}^\times \cong SL_2(\mathbb{C})/\{\pm 1\},$$

and we win!

Notice that being able to take square roots in $\mathbb{C}$ was an essential part of our proof. What if we let $F = \mathbb{R}$? Then we have the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then $\det(A) = -1$, and for all $\lambda \in \mathbb{R}^\times$, we have

$$\det(\lambda A) = \lambda^2 \det A = -\lambda^2 < 0.$$

In particular, there is no $\mathbb{R}^\times$ scaling of A to get positive determinant, much less determinant 1, so that $A \notin SL_2(\mathbb{R}) \cdot \mathbb{R}^\times$, and so Equation 3 fails. The most we can say here is that (applying the 4th ismomorphism theorem 1(e)(i) above) is that:

$$SlL_2(\mathbb{R})/\{\pm I\} \leq PGL_2(\mathbb{R}), \tag{4}$$

and similarly for any field F. One should notice that the existence of square roots was the precise obstruction to this being an equality. I encourage you to work out the details for a general field F, the analog of Equation 4 always holds, and is an equality if and only if every element of F is a square: that is $F^\times = (F^\times)^2$. □