Homework Assignment 7 Solutions

1. Let G be a group and let $H, K \leq G$ be subgroups. Recall that we defined the set:

$$HK = \{hk : h \in H, k \in K\} \subseteq G.$$

The second isomorphism theorem relied on the following two facts, which you will now verify.

(a) Show that HK is a subgroup of G if and only if $HK = KH$.

Proof. Suppose HK is a subgroup of G. As $K, H \leq HK$, and HK is closed under multiplication, we see that $KH \subseteq HK$. For the reverse inclusion, fix $hk \in HK$ where $h \in H$ and $k \in K$. We'd like to show that $hk \in KH$. Since HK is closed under inversion, $(hk^{-1}) \in HK$, so in particular $(hk^{-1}) = \hat{h}\hat{k}$ for some $\hat{h} \in H$ and $\hat{k} \in K$. But then $hk = (\hat{h}\hat{k})^{-1} = \hat{k}^{-1}\hat{h}^{-1} \in KH$, as needed.

For the converse, suppose that $HK = KH$. We must show that HK is nonempty, and closed under multiplication and inversion. Nonemptyness follows because both H and K are nonempty. Fix $hk \in HK$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ showing closure under inverses. Now fix $h_1k_1, h_2k_2 \in HK$. We observe that $k_1h_2 \in KH = HK$ so that $k_1h_2 = \hat{h}\hat{k} \in HK$. With this in hand we can compute the product:

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(\hat{h}\hat{k})k_2 = (h_1\hat{h})(\hat{k}k_2) \in HK,$$

as desired. □

(b) Use part (a) to show that that if $H \leq N_G(K)$, then HK is a subgroup of G. Explain why this means that if either H or K are normal subgroups, then $HK \leq G$.

Proof. The fact that $H \leq N_G(K)$ means that $hKh^{-1} = K$ for all $h \in H$. Multiplying on the right by h gives $hK = Kh$, and taking the union over all $h \in H$ gives $HK = KH$, so that HK is a subgroup by part (a). In particular, if K is normal, than it is trivial that $H \leq N_G(K) = G$, and symmetrically if H is normal. □

2. Let G be a group, and $M, N \trianglelefteq G$ normal subgroups such that $MN = G$. Use the first and second isomorphism theorems to establish the following facts.

(a) Show $G/(M \cap N) \cong (G/M) \times (G/N)$

Proof. We build a homomorphism $\pi : G \to (G/M) \times (G/N)$ via the rule $\pi(g) = (gM, gN)$. This is clearly a homomorphism since:

$$\pi(xy) = (xyM, xyN) = (xMyM, xNyN) = (xM, xN)(yM, yN) = \pi(x)\pi(y).$$

We now observe that π is surjective. Fix (xM, yN) in the target. Since $MN = G$, there is $m \in M$ and $n \in N$ such that $x^{-1}y = mn$. Solving one gets $xm = yn^{-1}$, call this value g. Then:

$$\pi(g) = (gM, gN) = (xmM, yn^{-1}N) = (xM, yN).$$

Finally, notice that the kernel of π is the set of $g \in G$ such that $gM = M$ and $gN = N$. But this is precisely $M \cap N$. Therefore, the first isomorphism theorem gives the result. □

(b) Suppose further that $M \cap N = \{1\}$. Show that $G \cong M \times N$.

Proof. The following lemma is perhaps obvious, but we include a proof for completeness.

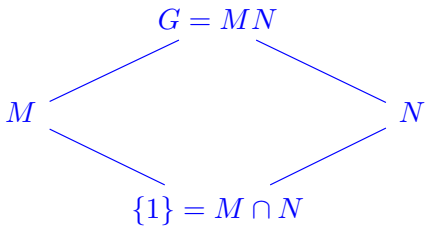
Lemma 1. *Suppose $H_1 \cong H_2$ and $K_1 \cong K_2$. Then $H_1 \times K_1 \cong H_2 \cong K_2$.*

Proof. Let $\varphi : H_1 \to H_2$ and $\psi : K_1 \to K_2$ be isomorphisms. Then we build:

$$\begin{array}{rccc} \varphi \times \psi : H_1 \times K_1 & \longrightarrow & H_2 \times K_2 \\ (h, k) & \mapsto & (\varphi(h), \psi(k)). \end{array}$$

It is easy to verify that $\varphi \times \psi$ is a homomorphism and that $(\varphi \times \psi)^{-1} = \varphi^{-1} \times \psi^{-1}$. □

Now to prove the result, we consider the diamond:



By the second isomorphism theorem we have $G/M \cong N$ and $G/N \cong M$. Therefore, the result follows from the following chain of isomorphisms, where the first is part (a), and the second is the lemma.

$$G \cong (G/M) \times (G/N) \cong N \times M.$$

□

3. We continue 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. We first observe that $\pi^{-1}(H)$ contains N, since for $n \in N$, we have $\pi(n) = 1 \in H$ so that $n \in \pi^{-1}(H)$. This also gives nonemptyness of the preimage of H, since N is a subgroup and therefore nonempty. To complete the proof we use the subgroup criterion of HW4#2(a), observing that 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 $\pi^{-1}(H)$ is indeed a subgroup. □

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

Proof. One could show this directly. Perhaps more efficient is to observe that one can restrict π to H to get a homomorphism $\pi|_H : H \to G/N$, whose image is precisely $\pi(H)$, and is therefore a subgroup by HW4#4(b). □

(c) These constructions do not in general 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. This means showing that $\pi(\pi^{-1}(\overline{H})) = \overline{H}$ for every $\overline{H} \leq G/N$, and that $\pi^{-1}(\pi(H)) = H$ for every $H \leq G$ containing N.

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 $\overline{H} \subseteq \pi(\pi^{-1}(\overline{H}))$.

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. 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 $\pi^{-1}(\overline{H}) \leq \pi^{-1}(\overline{K})$, because 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 HW5#1(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).*

4. By Cayley's theorem, the group Q_8 from HW6 Problem 5 is isomorphic to a subgroup of S_8. Let's write down such a subgroup explicitly!

(a) Label $\{1, -1, i, -i, j, -j, k, -k\}$ as the numbers $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Then the action of Q_8 on itself by left multiplication gives an injective map $Q_8 \to S_8$. Write the permutation representations for -1 and i as elements $\sigma_{-1}, \sigma_i \in S_8$, and verify that $\sigma_i^2 = \sigma_{-1}$. (Using the multiplication table from HW6 Problem 5 may make this easier).

Proof. Let's first compute σ_{-1}.

$$\begin{array}{rcl} -1 * 1 = -1 & \leftrightarrow & \sigma_{-1}(1) = 2 \\ -1 * -1 = 1 & \leftrightarrow & \sigma_{-1}(2) = 1 \\ -1 * i = -i & \leftrightarrow & \sigma_{-1}(3) = 4 \\ -1 * -i = i & \leftrightarrow & \sigma_{-1}(4) = 3 \\ -1 * j = -j & \leftrightarrow & \sigma_{-1}(5) = 6 \\ -1 * -j = j & \leftrightarrow & \sigma_{-1}(6) = 5 \\ -1 * k = -k & \leftrightarrow & \sigma_{-1}(7) = 8 \\ -1 * -k = k & \leftrightarrow & \sigma_{-1}(8) = 7 \end{array}$$

Thus σ_{-1} swaps 1 and 2, 3 and 4, 5 and 6, 7 and 8. That is:

$$\sigma_{-1} = (12)(34)(56)(78) \in S_8.$$

Let's do a similar computation for σ_i.

$$\begin{array}{rcl} i * 1 = i & \leftrightarrow & \sigma_i(1) = 3 \\ i * -1 = -i & \leftrightarrow & \sigma_i(2) = 4 \\ i * i = -1 & \leftrightarrow & \sigma_i(3) = 2 \\ i * -i = 1 & \leftrightarrow & \sigma_i(4) = 1 \\ i * j = k & \leftrightarrow & \sigma_i(5) = 7 \\ i * -j = -k & \leftrightarrow & \sigma_i(6) = 8 \\ i * k = -j & \leftrightarrow & \sigma_i(7) = 6 \\ i * -k = j & \leftrightarrow & \sigma_i(8) = 5 \end{array}$$

Thus σ_i takes 1 to 3 to 2 to 4 to 1, while taking 5 to 7 to 6 to 8 and back to 5. Thus we have:

$$\sigma_i = (1324)(5768) \in S_8.$$

Next we compute the square of σ_i by hand, using in the first equality that disjoint cycles commute.

$$\begin{array}{rcl} (\sigma_i)^2 & = & (1324)^2(5768)^2 \\ & = & (1324)(1324)(5768)(5768) \\ & = & (12)(34)(56)(78). \end{array}$$

□

(b) Use the generators from HW6 Problem 5(b) to give two elements of S_8 which generate a subgroup $H \leq S_8$ isomorphic to Q_8.

Proof. Since i and j generate Q_8, the permutations σ_i and σ_j generate the isomorphic subgroup of S_8. Thus we must also compute σ_j like we did for i and -1 in part (a).

$$\begin{aligned} j*1=j &\leftrightarrow \sigma_j(1)=5\\ j*-1=-j &\leftrightarrow \sigma_j(2)=6\\ j*i=-k &\leftrightarrow \sigma_j(3)=8\\ j*-i=k &\leftrightarrow \sigma_j(4)=7\\ j*j=-1 &\leftrightarrow \sigma_j(5)=2\\ j*-j=1 &\leftrightarrow \sigma_j(6)=1\\ j*k=i &\leftrightarrow \sigma_j(7)=3\\ j*-k=-i &\leftrightarrow \sigma_j(8)=4 \end{aligned}$$

Therefore we get:

$$\sigma_j = (1526)(3847).$$

Thus we have:

$$Q_8 \cong \langle \sigma_i, \sigma_j \rangle = \langle (1324)(5768), (1526)(3847) \rangle \leq S_8.$$

□

5. Let G be a group. Let $[G,G] = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$.

   (a) Show that $[G,G]$ is a normal subgroup of G.

   Proof. Notice that $[G,G]$ is not the set of elements of the form $x^{-1}y^{-1}xy$, it is the subgroup *generated* by elements of that form. In particular, it is automatically a subgroup, and all we must do is verify normality. Let's first prove a lemma.

   Lemma 2. *Let H be a group and consider a subset S. To see that $\langle S \rangle$ is normal it suffices to show $hsh^{-1} \in \langle S \rangle$ for all $h \in H$ and $s \in S$.*

   Proof. An arbitrary element in $\langle S \rangle$ looks like $s = s_1 s_2 \cdots s_n$ for s_i or s_i^{-1} in S. Then by assumption $gs_ig^{-1} \in \langle S \rangle$, so that:

   $$gsg^{-1} = g(s_1 s_2 \cdots s_n)g^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_ng^{-1}) \in \langle S \rangle.$$

   □

   Therefore for g and a commutator $x^{-1}y^{-1}xy$, we notice:

   $$g(x^{-1}y^{-1}xy)g^{-1} = gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} = (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}),$$

   is also a commutator. Therefore the subgroup is normal. □

   (b) Show that $G/[G,G]$ is abelian.

   Proof. We must show that the cosets $xy[G,G]$ and $yx[G,G]$ are equal. But $x^{-1}y^{-1}xy \in [G,G]$ so that

   $$xy = yx(x^{-1}y^{-1}xy) \in yx[G,G].$$

   Since the cosets form a partition, we are done. □

$[G,G]$ is called the *commutator subgroup* of G, and $G/[G,G]$ is called the *abelianization* of G, denoted G^{ab}. The rest of this exercise explains why.

(c) Let $\varphi : G \to H$ be a homomorhism with H abelian. Show $[G,G] \subseteq \ker \varphi$.

Proof. It suffices to show that every element $x^{-1}y^{-1}xy \in G$ is in the kernel of φ, since then $[G,G]$ is generated by elements in the kernel. But then:

$$\varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) = \varphi(x)\varphi(x)^{-1}\varphi(y)^{-1}\varphi(y) = 1,$$

as H is abelian. (Notice we also just showed that the commutator subgroup of an abelian group is always the trivial subgroup). □

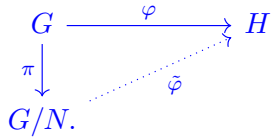
(d) Conclude that for H an abelian group there is a bijection:

$$\{ \text{ Homomorphisms } \varphi : G \to H \ \} \iff \{ \text{ Homomorphisms } \tilde{\varphi} : G^{\text{ab}} \to H \ \}$$

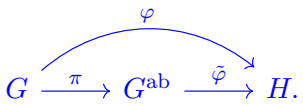
Hint. *Recall the technique of passing to the quotient described in the 5/3 lecture.*

Proof. We remind the reader of the statement of "Passing to the Quotient."

Lemma 3 (Passing to the Quotient)**.** *Let $N \trianglelefteq G$ be a normal subgroup, and $\varphi : G \to H$ a homomorphism. If $N \leq \ker \varphi$, then there is a unique homomorphism $\tilde{\varphi} : G/N \to H$ such that $\tilde{\varphi} \circ \pi = \varphi$, defined by the rule $\tilde{\varphi}(gN) = \varphi(g)$. This is summarized by the following diagram.*



With this lemma we prove part (d). In the righthand direction we define a function Φ which takes a map $\varphi : G \to H$ to the unique map $\tilde{\varphi}$ from the lemma, which exists because $[G,G] \leq \ker \varphi$ by part (c). In the other direction define Ψ which takes a map $\tilde{\varphi}$ to the composition $\varphi = \tilde{\varphi} \circ \pi$:



We must prove these processes are inverses to eachother. But this is obvious. $\Psi \circ \Phi(\varphi) = \tilde{\varphi} \circ \pi = \varphi$ by definition, and $\Phi \circ \Psi(\tilde{\varphi}) = \Phi(\tilde{\varphi} \circ \pi) = \tilde{\varphi}$ by the uniqueness of $\tilde{\varphi}$.
We make a remark that this is a sort of *universal property*, in that G^{ab} is the universal abelianization of G. I won't get into precisely what this means at the moment, but it can be understood via the slogan: Maps from G to abelian things are the same as maps from G^{ab} to abelian things. □

6. Let's now compute D_{2n}^{ab}. We should begin computing $xyx^{-1}y^{-1}$. There are 3 cases.

(a) Compute $x^{-1}y^{-1}xy$ in each of the following 3 cases. (*Hint:* HW2#9(e) gives the inverse for a reflection.)

(i) x, y both reflections. So $x = sr^i$ and $y = sr^j$.

Proof. Since reflections always have order two, we have $x^{-1} = x$ and $y^{-1} = y$. That is:

$$x^{-1}y^{-1}xy = (sr^i)(sr^j)(sr^i)(sr^j) = r^{j-i}r^{j-i} = r^{2(j-i)}$$

As i and j vary we collect all even powers of r. □

(ii) x a reflection and y not a reflection. So $x = sr^i$ and $y = r^j$.

Proof. In this case $x^{-1} = x$, but that is not true for y. We compute

$$x^{-1}y^{-1}xy = (sr^i)(r^{-j})(sr^i)(r^j) = (sr^{i-j})(sr^{i+j}) = r^{2j},$$

and as above we collect precisely the even powers of r. □

(iii) Neither x nor y are reflections. So $x = r^i$ and $y = r^j$.

Proof. Here x and y commute so their commutator is 1. □

(b) Prove that $[D_{2n}, D_{2n}] = \langle r^2 \rangle$. If n is odd one could choose another generator. What is it?

Proof. We saw in part (a) that the commutators of D_{2n} are precisely the even powers of r, proving the first statement. If n is odd, then $(n+1)/2$ is an integer and we can compute

$$(r^2)^{(n+1)/2} = r^{n+1} = r,$$

so that in fact the commutator subgroup is $\langle r \rangle$. □

(c) Now prove that D_{2n}^{ab} is either V_4 or Z_2 depending on whether n is odd or even. Note that since this is so small we should interpret this as suggesting that D_{2n} is far from abelian.

Proof. Note that:

$$|D_{2n}^{\text{ab}}| = |D_{2n}/|[D_{2n}, D_{2n}]| = |D_{2n}|/|[D_{2n}, D_{2n}]|.$$

If n is odd, then $|[D_{2n}, D_{2n}]| = n$ which is half the order of D_{2n}. Thus $|D_{2n}^{\text{ab}}| = 2$, and so it must be Z_2 by TH1#4(a).

If n is even then $|[D_{2n}, D_{2n}]| = n/2$, a quarter of the order of D_{2n}, and so $|D_{2n}^{\text{ab}}| = 4$ so it must be Z_4 or V_4 by TH1#4(d). To see it is V_4 we will show every element has order 2. The cosets are represented by r, s, and sr. The latter two have order two already in D_{2n}, so it remains to show that the coset represented by r does too, but its square is r^2 which generates the commutator subgroup. Since every element of D_{2n}^{ab} has order 2, it must be the group V_4. □

Let F be a field. The general linear group $GL_n(F)$ from HW6 Problem 7 has lots of interesting subgroups and quotients, which we study in the following problem. You may use the following fact without proof, as it is a standard result of linear algebra.

Proposition 1. *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.*

7. (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:

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

To check it is a homomorphism observe that:

$$\varphi(\lambda)\varphi(\tau) = (\lambda I)(\tau I) = (\lambda\tau)I = \varphi(\lambda\tau),$$

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

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

(*Hint:* Use the First Isomorphism Theorem and Proposition 1)

Proof. By Proposition 1 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 HW6 Problem 7(b). □

(d) Compute $|SL_2(\mathbb{F}_p)|$ (*Hint*, between 7(b) and HW6 Problem 7(d) 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 HW6 Problem 7(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.

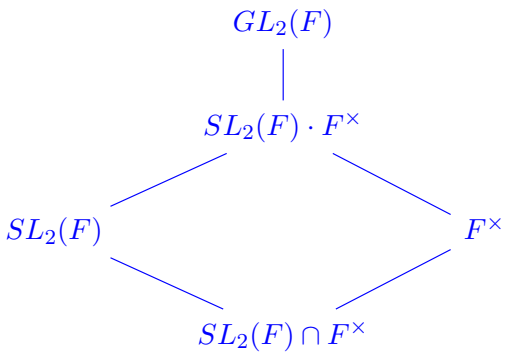
Proof. Notice that $I \in SL_n(F)$ always. On the other hand, $\det(-I) = (-1)^n$, which is 1 if and only if n is even. □

(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.



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 $\det(A) = d \neq 0$. 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 isomorphism theorem 3(e)(i) above) is that:

$$SL_2(\mathbb{R})/\{\pm I\} \leq PGL_2(\mathbb{R}), \tag{4}$$

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 $F^\times = (F^\times)^2$. □