Homework Assignment 6

Due Friday, March 6

1. There is an absolute value on the complex numbers given by $||a + bi|| = \sqrt{a^2 + b^2}$, where we use $|| \cdot ||$ rather than $| \cdot |$ so not confuse notation with order of a group element. Let $\mathbb{S}^1 = \{z \in \mathbb{C} : ||z|| = 1\}$. This is called the *circle group*.

(a) Show that $|| \cdot || : \mathbb{C}^\times \to \mathbb{R}^\times$ is a homomorphism.

Proof. We must show that for $z, w \in \mathbb{C}^\times$, we have $||z|| \cdot ||w|| = ||zw||$. Let $z = a + bi$ and $w = c + di$. Then

$$zw = (a + bi)(c + di) = ac - bd + (ad + bc)i$$

Then we compute:

$$\begin{aligned} ||z|| \cdot ||w|| &= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\ &= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2} \end{aligned}$$

and

$$\begin{aligned} ||zw|| &= \sqrt{(ac - bd)^2 + (ad + bc)^2} \\ &= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} \\ &= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2}, \end{aligned}$$

and observe that they are equal. □

(b) Show that the circle group is a normal subgroup of the multiplicative group $\mathbb{C}^\times$.

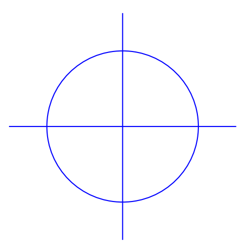
Proof. By definition we have:

$$\ker(|| \cdot ||) = \{z \in \mathbb{C}^\times : ||z|| = 1\} = \mathbb{S}^1,$$

so that the circle group is the kernel of a homomorphism and is therefore a normal subgroup (recall we proved in class that normal subgroups are precisely the kernels of homoromorphisms, a source for this result is Dummit and Foote proposition 3.1.7). □

(c) Draw the graph of the circle group in the complex plane. Justify your answer.

Proof. The point in the complex plane corresponding to $z = x + iy$ is the point (x, y). So $||z|| = \sqrt{x^2 + y^2} = 1$ is precisely saying that the point lies on the circle of radius 1.



□

(d) Show that $\varphi : \mathbb{R} \to \mathbb{S}^1$ defined by the rule $\varphi(x) = e^{2\pi i x}$ is a surjective homomorphism (where the binary operation on $\mathbb{R}$ is addition).

Proof. To see this is a homomorphism notice that:

$$\varphi(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x + 2\pi i y} = e^{2\pi i x} e^{2\pi i y} = \varphi(x)\varphi(y).$$

To see that this lands in $\mathbb{S}^1$ we recall that:

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

so that:

$$||e^{i\theta}|| = ||\cos\theta + i\sin\theta|| = \sqrt{\cos^2\theta + \sin^2\theta} = 1.$$

Also notice that $e^{i\theta}$ is therefore the point on $\mathbb{S}^1$ making an angle of θ with the x-axis. In particular, if z is any point on $\mathbb{S}^1$, we can measure its angle θ with the x-axis. Letting $r = \theta/2\pi$ we have

$$\varphi(r) = e^{2\pi i\theta/2\pi} = e^{i\theta} = z,$$

so that φ is surjective. □

For completeness, we include the proof of the identity we use (although I do not expect you to prove it).

Lemma 1. $e^{i\theta} = \cos\theta + i\sin\theta$

Proof. The Taylor expansion of the left hand side at 0 follows:

$$e^{i\theta} = \left(1 + (i\theta) + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \cdots\right).$$

We also taylor expand the righthand side of the equation term by term:

$$\cos\theta = \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \frac{\theta^6}{6!} + \cdots\right)$$

and,

$$i\sin\theta = i\left(\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \frac{\theta^7}{7!} + \cdots\right).$$

Since $i^2 = -1$ first is clearly the sum of the second two. □

This has the following famous corollary that is hard to skip at this point. It is derived by letting $\theta = \pi$ in the lemma above.

Corollary 1. $e^{i\pi} + 1 = 0$.

(e) Deduce that the additive quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathbb{S}^1$

Proof. By the first isomorphism theorem, it suffices to show that the kernel of φ from part (d) is precisely $\mathbb{Z}$. But we should notice that $e^{i\theta} = 1$ if and only if the angle θ goes along the positive x axis, that is if θ is a multiple of 2π (you could also deduce this noticing that $\sin\theta = 0$ and $\cos\theta = 1$). Thus $\varphi(r) = 1$ precisely when $2\pi r$ is a multiple of 2π, that is precisely when r is an integer, so we win. □

2. A root of unity ξ is a complex number such that $\xi^n = 1$ for some positive integer n. The set of roots of unity is often denoted by $\mu\!\!\!/$.

   (a) ± 1 are roots of unity. Give 3 more examples of roots of unity.

   Proof. Notice that $i^4 = (i^2)^2 = (-1)^2 = 1$ so that i is a root of unity, and similary so is $-i$. Finally, consider $\omega = e^{2\pi i/3}$. Notice that by the lemma this is the complex number $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Then $\omega^3 = e^{2\pi i} = 1$. □

   (b) Show that if ξ is a root of unity, then $||\xi|| = 1$.

   Proof. Since ξ is a root of unity we have $\xi^n = 1$ for some positive integer n. Since $||\cdot||$ is a homomorphism we therefore have:

$$||\xi||^n = ||\xi^n|| = ||1|| = 1.$$

   Therefore $||\xi||$ is a positive real number whose nth power is 1. The only such number is 1. □

   (c) Show that $\mu\!\!\!/ = (\mathbb{S}^1)^{\text{tors}}$ (recall the definition from HW 4 Problem 2(b)). Deduce that $\mu\!\!\!/$ is a subgroup of $\mathbb{S}^1$.

   Proof. Suppose $\xi \in \mu\!\!\!/$. Then from part (b) we have that $\xi \in \mathbb{S}^1$, but also since $\xi^n = 1$ we have that the order of ξ is less than n, and in particular finite. Thus ξ is a torsion element of $\mathbb{S}^1$. Since ξ was arbitrary, we have $\mu\!\!\!/ \subseteq (\mathbb{S}^1)^{\text{tors}}$. Conversely, if z is a torsion element of the circle, it has finite order $n < \infty$. Then in particular $z^n = 1$ so that z is a root of unity. This show $(\mathbb{S}^1)^{\text{tors}} \subseteq \mu\!\!\!/$ so that they are equal.

   Since $\mathbb{S}^1$ is abelian (its group operation is complex multiplication which is commutative), the torsion subset is a subgroup, so that $\mu\!\!\!/ \leq \mathbb{S}^1$. □

3. Consider the additive group quotient $\mathbb{Q}/\mathbb{Z}$.

   (a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ has exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.

   Proof. For $a \in \mathbb{Q}$ its coset is $a + \mathbb{Z} = \{a + n : n \in \mathbb{Z}\}$. We know that $m \leq a < m + 1$ for some integer m, so that $0 \leq a - m < 1$. But also $a - m \in a + \mathbb{Z}$, so we have exhibited a coset representative in the range $0 \leq q < 1$ and therefore there must be at least one.

   To show there is *at most* 1, suppose that $q, q' \in a + \mathbb{Z}$ with $0 \leq q \leq q' < 1$. Then $q' - q \in \mathbb{Z}$, but also $0 \leq q' - q < 1$, so that $q' - q = 0$.

   (Note that in the last paragraph we used that if q, q' represent the same coset, their difference must be in the subgroup. We showed this in class, for a reference see Dummit and Foote Proposition 3.1.4). □

   (b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, but that there are elements of arbitrary large order.

Proof. Pick an element of $\mathbb{Q}/\mathbb{Z}$, and represent it as $a + \mathbb{Z}$. Then $a = m/n$ for some $m, n \in Z$. Thus $n \cdot (a + \mathbb{Z}) = na + \mathbb{Z} = m + \mathbb{Z}$, but as $m \in \mathbb{Z}$ this means that it is the trivial coset $\mathbb{Z}$. In particular, $a + \mathbb{Z}$ has order $\leq n < \infty$.

To exhibit an element of arbitrarily large order we fix any large integer N. We must exhibit a coset of order N. I claim $1/N + \mathbb{Z}$ works. Indeed, for $m > 0$ we have $m \cdot (1/N + \mathbb{Z})$ is the trivial coset if and only if m/N is an integer, if and only if $N | m$. Therefore the order of $1/N + \mathbb{Z}$ is precisely N. □

(c) Show that $\mathbb{Q}/\mathbb{Z} = (\mathbb{R}/\mathbb{Z})^{\text{tors}}$. Conclude that $\mathbb{Q}/\mathbb{Z} \cong \mu$.

Proof. Let $\iota : \mathbb{Q} \to \mathbb{R}$ be the homomorhism given by including $\mathbb{Q}$ as a subgroup of $\mathbb{R}$, and let $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ be the natural projection. Then $\pi \circ \iota : \mathbb{Q} \to \mathbb{R}/\mathbb{Z}$ is a homomorphism with kernel $\mathbb{Z}$. Thus by the first isomorphism theorem it induces an injective map $\mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$, which is the obvious map $a + \mathbb{Z} \mapsto a + \mathbb{Z}$. This identifies $\mathbb{Q}/\mathbb{Z}$ as a subgroup of $\mathbb{R}/\mathbb{Z}$ consisting of cosets with representatives in $\mathbb{Q}$. Part (b) immediately implies that $\mathbb{Q}/\mathbb{Z} \subseteq (\mathbb{R}/\mathbb{Z})^{\text{tors}}$. To show the reverse inclusion, suppose $a + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ is a torsion coset. Thus it has a multiple which is the trivial coset. Equivalently, a multiple of a must be an integer. But this implies $a \in \mathbb{Q}$, so that $a + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, and therefore $(\mathbb{R}/\mathbb{Z})^{\text{tors}} \subseteq \mathbb{Q}/\mathbb{Z}$, so they are equal.

The second statement follows immediately from the following lemma.

Lemma 2. *Let $\varphi : G \to H$ be an isomorphism. Then φ restricts to a bijection $G^{\text{tors}} \to H^{\text{tors}}$, which is an isomorphism if G is abelian.*

Proof. In HW3 Problem 1(e) we showed $|\varphi(g)| = |g|$, so that if $g \in G^{\text{tors}}$, its image $\varphi(g)$ is in H^{tors}. The same can be said for φ^{-1}. So the restriction $\varphi : G^{\text{tors}} \to H^{\text{tors}}$ has inver φ^{-1} so is a bijection. If G is abelian, so is H, and φ restricts to a bijective homomorphism between the subgroups G^{tors} and H^{tors}. □

With this in hand, we see that the ismomorphism $\mathbb{R}/\mathbb{Z} \to \mathbb{S}^1$ restricts to an isomorphism between their torsion subgroups, which are $\mathbb{Q}/\mathbb{Z}$ and μ respectively. □

4. 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 $\pi^{-1}(H)$ 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, 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 $y = \pi(b)$. Then

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

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

(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 $H = 4\mathbb{Z} \leq N$, so that $\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the projection. Then $\pi(N) = \pi(H) = \{\overline{0}\}$, so that the identification $H \mapsto \pi(H)$ is not injective. In fact, as the following exercise shows, this is the only kind of thing that can go wrong. $\square$

(d) If we restrict our attention to certain subgroups of G we do get a bijection. Indeed, show that there is 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. In the righthand direction we have $\varphi : H \mapsto \pi(H)$. In the reverse direction we have $\psi : \overline{H} \mapsto \pi^{-1}(\overline{H})$. We showed these are well defined functions in parts (a) and (b), so it remains to show they are inverses to eachother.
First notice that

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

To show the reverse incusion, fix some $\overline{h} \in \overline{H}$, there is some $h \in G$ usch 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 $\overline{h} = \pi(h) \in \pi(\pi^{-1}(\overline{H}))$. Thus we have show that $\varphi \circ \psi$ is the identity.
In the other direction, notice that

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

To show the reverse inclusion, fix some $g \in G$ and suppose that $\pi(g) = \pi(h)$ for some $h \in H$. Then $\pi(hg^{-1}) = \pi(g)\pi(h)^{-1} = 1$, so that $gh^{-1} \in N$. But 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 so $\psi \circ \varphi$ is the identity as well. In particullar, they are inverses to eachother, and induce the diesired bijection. $\square$

5. Let G be a group and $Z(G)$ its center.

(a) Show that $Z(G)$ is a normal subgroup.

Proof. Fix $z \in Z(G)$ and $g \in G$. It suffices to show $gzg^{-1} \in Z(G)$. But everything in G commutes with everything in $Z(G)$, so $gzg^{-1} = gg^{-1}z = z \in Z(G)$, so we are done. $\square$

(b) Show that if $G/Z(G)$ is cyclic, then G is abelian.

Proof. If $G/Z(G)$ is cyclic then we can fix a generator: $G/Z(G) = \langle xZ(G)\rangle$. Then the cosets $x^iZ(G)$ for $i \in \mathbb{Z}$ form a partition of G. In particular, fix $a, b \in G$. Then $a = x^iz$ and $b = x^jw$ for $z, w \in Z(G)$. Therefore we can leverage that we can free commute with z and w, and x^i and x^j commute with eachother to conclude that

$$ab = x^izy^jw = zx^ix^jw = zx^jx^iw = x^jzwx^i = x^jwzx^i = x^jwx^iz = ba.$$

Thus a and b commute, but since they were arbitrary we conclude that G is abelian. □

(c) Let p and q be prime numbers (not necessarily distinct), and G a group of order pq. Show that if G is not abelian, than $Z(G) = \{1\}$.

Proof. Since G is not abelian then $Z(G) \neq G$. If $Z(G) \neq 1$ then by Lagrange's theorem, $Z(G)$ has either order p or q. Assume without loss of generality that it has order q. Then $|G/Z(G)| = |G|/|Z(G)| = q$, so that $G/Z(G)$ has prime order and therefore must be cyclic (we proved this in class, for a reference see Dummit and Foote Corollary 3.2.10). But then by part (b) G must be abelian, a contradiction. Therefore $Z(G)$ must be 1. □

6. 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. So we need not show it is a subgroup. Lets first prove a lemma.

Lemma 3. *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 $s = s_1s_2\cdots s_n$ for s_i or s_i^{-1} in S. Then by assumption $gs_ig^{-1} \in \langle S\rangle$, so that:

$$gsg^{-1} = g(s_1s_2\cdots s_n)g^{-1} = (gs_1g^{-1})(gs_2g^{-1})\cdots(gs_ng^{-1}) \in \langle S\rangle.$$

□

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.

We concluded the proof above, but there is a slightly slicker way to see this, following from the next lemma.

Lemma 4. *Let $\varphi : H \to K$ is a homomorphism of groups. Then the image of a commutator is a commutator.*

Proof. This is immediate, as $\varphi(x^{-1}y^{-1}xy) = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y)$. □

Then we need only notice that for every $g \in G$, the conjugation map $\varphi_g : G \to G$ given by $\varphi_g(x) = gxg^{-1}$ is a homomorphism. Indeed,

$$\varphi_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi_g(x)\varphi_g(y).$$

Then we immediatly conclude that conjugating a commutator gives a commutator. □

(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. 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) Denote the natural projection to the quotient group by $\pi : G \to G^{\text{ab}}$. Prove that φ induces a unique homomorphism $\tilde{\varphi} : G^{\text{ab}} \to H$ such that $\pi \circ \tilde{\varphi} = \varphi$.

Proof. Since the kernel of φ contains the commutator subroup, this follows directly from the factorization lemma we proved in class. Since it isn't directly stated in the book we include it here for completeness.

Lemma 5 (Factoriaztion Lemma)**.** *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 $G/N \to H$ making the following diagram commute:*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & H \\ G/N. \arrow[ur, dotted, "\tilde{\varphi}"'] & \end{tikzcd}$$

Proof. If the diagram commutes, then we must have $\tilde{\varphi}(gN) = \tilde{\varphi}(\pi(g)) = \varphi(g)$, proving uniqueness. Therefore it suffices to show that the rule $\tilde{\varphi}(gN) = \varphi(g)$ is well defined if $N \leq \ker\varphi$. Suppose $g' \in gN$. Then $g'g^{-1} \in N$ so that $\varphi(g'g^{-1}) = 1$. Thus $\varphi(g') = \varphi(g)$ and so $\tilde{\varphi}$ is well defined. □

□

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

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

Proof. In the righthand direction we define a function Φ which takes a map $\varphi : G \to H$ to the unique map $\tilde{\varphi}$ from part (d). In the other direction define Ψ which takes a map $\tilde{\varphi}$ to the composition $\varphi = \tilde{\varphi} \circ \pi$:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[rr, bend left, "\varphi"] & G^{\mathrm{ab}} \arrow[r, "\tilde{\varphi}"] & H. \end{tikzcd}$$

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. $\square$

7. 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.

(i) x, y both reflections. So $x = sr^i$ and $y = sr^j$. Recall that reflections always have order 2.

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. $\square$

(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 computeL

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

and as above we collect precisely the even powers of r. $\square$

(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. $\square$

(b) Prove that $[D_{2n}, D_{2n}] = \langle r^2 \rangle$. If n is odd, there is 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 $\langle r \rangle$. $\square$

(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.

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. To see it is V_4 we must 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. $\square$

Bonus In Problem 1 we could have gone in a different direction after part (a). If you're interested, compose the complex absolute value with the log map to construct an isomorphism between $\mathbb{C}^\times/\mathbb{S}^1$ and the additive group $\mathbb{R}$. Describe in words the $\mathbb{S}^1$ cosets and how they correspond to elements of $\mathbb{R}$ (hint, it looks like a target!). I can't promise many extra points for this, but I do think it's a fun exercise.

Proof. We have the composition as $\mathbb{S}^1$ is the kernel of the absolute value map, we have an isomorphism between $\mathbb{C}^\times/\mathbb{S}^1$ and the image of the absolute value map. Notice that $||a + bi|| = \sqrt{a^2 + b^2}$ is always a positive real number. Conversely, if $r \in \mathbb{R}$ then viewing it as a complex number $r + 0i$ we have $||r|| = r$, so that the image of the absolute value map is precisely $R_{>0}$. In particular, the first isomorphism theorem tells us $\mathbb{C}^\times/\mathbb{S}^1 \cong \mathbb{R}_{>0}$ where the binary operation on the latter is multiplication. But recall from class that $\log : (\mathbb{R}_{>0}, \times) \to (\mathbb{R}, +)$ is an isomorphism, so that in fact $\mathbb{C}^\times/\mathbb{S}^1 \cong R$.

The fibers of this map are easier to understand before taking log. Indeed, $|| \cdot ||^{-1}(r)$ is precisely the circle of radius r centered at 0 in the complex plane. So the cosets are precisely the circles, and the relationship to the positive real numbers is the circle of radius r corresponds to r. $\square$