Homework 2

1. Let G be a group, $H \subset G$ be a subgroup, and $g \in G$. We will show $gHg^{-1} = \{ghg^{-1} : h \in H\}$ is a subgroup.

   It contains the identity since $geg^{-1} = gg^{-1} = e$.

   It contains inverses: let gag^{-1} be some element of gHg^{-1}, with $a \in H$. Then since H is a subgroup, $a^{-1} \in H$, and $ga^{-1}g^{-1} \in gHg^{-1}$ is the inverse of gag^{-1} since $gag^{-1}ga^{-1}g^{-1} = gaa^{-1}g^{-1} = e$.

   Finally, gHg^{-1} is closed under multiplication since for $gag^{-1}, gbg^{-1} \in gHg^{-1}$, $gag^{-1}gbg^{-1} = gabg^{-1}$. As H is a subgroup, we have $ab \in H$ and thus $gabg^{-1} \in gHg^{-1}$.

   Now we show that gHg^{-1} is isomorphic to H. I claim the map $\varphi : H \to gHg^{-1}$ defined by $a \mapsto gag^{-1}$ is an isomorphism of subgroups. It is a group homomorphism since $\varphi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \varphi(a)\varphi(b)$. It is injective: suppose $\varphi(a) = e$. Then $gag^{-1} = e$, and thus $a = g^{-1}eg = e$. It is surjective: choose any $gag^{-1} \in gHg^{-1}$. Then $\varphi(a) = gag^{-1}$. Thus φ is an isomorphism.

2. Let G be a group and H, K be proper subgroups of G such that $G = H \cup K$. We cannot have $H \subset K$ or $K \subset H$ since this would mean either $H = G$ or $K = G$, a contradiction.

   Then there exists some $h \in H$ such that $h \notin K$. For any $k \in K$, I claim that $hk \notin K$. Suppose it is. Then there is some $k' \in K$ such that $hk = k'$, and $h = k'k^{-1}$. Since K is a subgroup, this implies $h \in K$, a contradiction.

   There also exists $k \in K$ with $k \notin H$. Applying the above reasoning also to K, we have $hk \notin H$ and $hk \notin K$. But $hk \in G$, which contradicts that $G = H \cup K$. Then we are done.

   ———

   We now show that $\mathbb{Z} \oplus \mathbb{Z}$ is the union of three proper subgroups. Let

   $$A_1 = \langle (1,1), (0,2) \rangle, A_2 = \langle (2,2), (0,1) \rangle, A_3 = \langle (2,2), (1,0) \rangle,$$

   each subgroups generated by two elements. They are each proper subgroups: A_1 does not contain elements of the form $(a, a+1)$, A_2 does not contain elements of the form $(2a+1, b)$, and similarly A_3 does not contain elements $(a, 2b+1)$.

   I claim that $\mathbb{Z} \otimes \mathbb{Z}$ is the union of these three subgroups.

   Choose any $(x, y) \in \mathbb{Z} \oplus \mathbb{Z}$. If $x = 2a$ for some $a \in \mathbb{Z}$, we can express $(x, y) = (2a, 2a + b) = a(2,2) + b(0,1)$, where $b = y - x$. Then $(x, y) \in A_2$.

   If this is not the case, then if $y = 2b$ for some $b \in \mathbb{Z}$, we can write $(x, y) = (a + 2b, 2b) = a(1,0) + b(2,2)$, where $a = x - y$, and $(x, y) \in A_3$.

   Finally, if neither of these conditions are true, both x and y must be odd, and we have $y - x = 2a$ for some $a \in \mathbb{Z}$. Then we can write $(x, y) = (x, x + 2a) = x(1,1) + a(0,2)$, and $(x, y) \in A_1$

   We have shown that every element of $\mathbb{Z} \oplus \mathbb{Z}$ is an element of at least one of the three proper subgroups. Then $\mathbb{Z} \oplus \mathbb{Z} = A_1 \cup A_2 \cup A_3$ as sets.

3. Let A and B be groups with elements $a \in A$ and $b \in B$ and consider $(a, b) \in A \times B$. If either a or b has infinite order, the order of (a, b) must be infinite.

   Otherwise, let α and β be the orders of a and b, respectively, and $m = \operatorname{lcm}(\alpha, \beta)$, the least common multiple. Then $m = p\alpha = q\beta$ for some $p, q \in \mathbb{N}$, and $(a, b)^m = (a^m, b^m) = ((a^\alpha)^p, (b^\beta)^q) = (e, e)$. Since m is by definition the smallest element for which $a^m = b^m = e$, it must be the order of (a, b).

4. Let $G = \{e, a, b, c\}$ be a group of four elements with identity e. Suppose G has no element of order 4. We will not assume that the order of a subgroup divides the order of a group.

   Suppose a has order 3, so that $a^3 = e$. Then WLOG assume $a^2 = b$. $\langle a \rangle$ is a cyclic subgroup of G of order 3. I claim that the element ca is not in $\langle a \rangle$. If $ca = e$, then $c = a^2 = b$, a contradiction. If $ca = a$, then $c = e$, also a contradiction. Finally if $ca = a^2$, then $c = a$, also a contradiction, and we have shown $ca \notin \langle a \rangle$.

Then $ca = c$, but this is impossible since $a \neq e$. Then a is not order 3. The same argument holds for b and c.

Then each non identity element has order 2. We must have $ab = c$, since neither a nor b are the identity, and $ab = e$ implies $a = b$ which is impossible. Similarly, $ba = c$.

The same is true as well for the other products of nonidentity elements. This shows G is abelian, and we have completely determined the group structure of G.

5. Let $\mathbb{Q}$ be the rational numbers and let $A = \langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$ be a finitely generated subgroup.

   Let $m = \operatorname{lcm}(b_1, \ldots, b_n)$. Then $\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle = \frac{1}{m} \langle p_1 a_1, \ldots, p_n a_n \rangle$ for $p_1, \ldots, p_n \in \mathbb{Z}$.

   Now let $n = \gcd(p_1 a_1, \ldots, p_n a_n)$, so that $\frac{1}{m} \langle p_1 a_1, \ldots, p_n a_n \rangle = \frac{n}{m} \langle p_1 q_1, \ldots, p_n q_n \rangle$ again for some $q_1, \ldots, q_n \in \mathbb{Z}$.

   Then $\gcd(p_1 a_1, \ldots, p_n a_n) = n$ implies that

$$\gcd\left(\frac{p_1 a_1}{n}, \ldots, \frac{p_n a_n}{n}\right) = \gcd\left(p_1 q_1, \ldots, p_n q_n\right) = 1,$$

   and by Bezout's identity, there exist integers $r_1, \ldots, r_n$ such that $r_1 p_1 q_1 + \cdots + r_n p_n q_n = 1$. In other words, $1 \in \langle p_1 q_1, \ldots, p_n q_n \rangle$ and therefore $\langle p_1 q_1, \ldots, p_n q_n \rangle = \langle 1 \rangle$.

   Finally, we have

$$\left\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \right\rangle = \frac{n}{m} \langle p_1 q_1, \ldots, p_n q_n \rangle = \left\langle \frac{n}{m} \right\rangle$$

   and thus $\langle \frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n} \rangle$ is cyclic.

   Now we will show that there is a subgroup of $\mathbb{Q}$ which is not finitely generated. Let $A \subset \mathbb{Q}$ be the rational numbers whose denominator is a power of 2. We just showed that such a subgroup being finitely generated is equivalent to it being cyclic. Then we only need to show A has no generator.

   Suppose it does, and $A = \langle x \rangle$ for some $x \in \mathbb{Q}$. We must have $x \in A$, so $x = \frac{a}{2^b}$ for $a, b \in \mathbb{Z}$. Then there is some $c \in \mathbb{Z}$ such that $\frac{1}{2^{b+1}} = \frac{ca}{2^b}$, so $ca = \frac{1}{2}$ which is impossible if a and c are integers.

6. Let D_4 be the group generated by $S := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $R = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ under matrix multiplication.

   Since S and R have a determinate of ± 1, we know that any element of D_4 must also have a determinate of ± 1. Also, any matrix in this group must have entries ± 1 since S and R only contain these values. Then we can only have matrices of the form $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{smallmatrix}\right)$.

   We must also show that each of the 8 possibilities can be generated by S and R. We have

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$S^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad S^4 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad SR = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$S^2 R = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \qquad S^3 R = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

   It is nonabelian since $RS = S^3 R$ differs from SR above.

   Each element of D_4 permutes the vertices $(\pm 1, \pm 1)$ of the square. The linear maps are injective, and any vector $(\pm 1, \pm 1)$ is sent to another $(\pm 1, \pm 1)$. The first four elements above correspond to rotations about the origin. The next four correspond to reflection about $x = y$, reflection about $x = 0$, reflection about $y = -x$, and reflection about $y = 0$, respectively.

7. Let Q_8 be the group generated by the matrices $\mathbf{i} := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\mathbf{j} := \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$, where $i = \sqrt{-1}$. We have relations $\mathbf{i}^4 = \mathbf{j}^4 = e$, and $\mathbf{i}^2 = \mathbf{j}^2$, as well as $\mathbf{ij} = \mathbf{ji}^3$ and $\mathbf{ji} = \mathbf{i}^3\mathbf{j}$.

   From the last relation, we can conclude that any element of Q_8 is of the form $\mathbf{i}^a\mathbf{j}^b$. This is because for any combination of elements $\mathbf{i}$ and $\mathbf{j}$, we can move all the $\mathbf{i}'s$ to the right as many times as needed, gaining exponents each shift. Also, $a, b \in \{1, 2, 3, 4\}$ because of the first relation.

   Note that the first and second relations imply that $\mathbf{i}^2\mathbf{j}^2 = e$. Then we can rewrite $\mathbf{i}^a\mathbf{j}^b = \mathbf{i}^{a-2}\mathbf{a}^2\mathbf{j}^2\mathbf{j}^{b-2} = \mathbf{i}^{a-2}\mathbf{j}^{b-2}$. This imposes a restriction on the total number of elements $\mathbf{i}^a\mathbf{j}^b$ so that there can be at most 8, since 8 of the possibilities are equal to 8 others.

   We can also write out 8 elements:

$$\mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \mathbf{i}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\mathbf{i}^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \mathbf{i}^4 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad \mathbf{j}^3 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$
$$\mathbf{ij} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad \mathbf{ji} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

   These these must be the 8 elements. Q_8 is nonabelian since $ij \neq ji$.

   Note that D_4 has 3 elements of order 2, listed above as S^2, R, and S^3R, while the only element of Q_8 which has order 2 is $\mathbf{i}^2$. Then these groups are not isomorphic.