(worked with Joseph Sullivan, Gahl Shemy)

1 Exercise I.34

(a) Let n be an even positive integer. Show that there exists a group of order $2n$, generated by two elements σ, τ such that $\sigma^n = e = \tau^2$, and $\sigma\tau = \tau\sigma^{n-1}$. This group is called the **dihedral group**.

Proof. We have a group presentation

$$D_{2n} = \langle \sigma, \tau \mid \sigma^n = \tau^2 = e, \sigma\tau = \tau\sigma^{n-1} \rangle.$$

The relation $\sigma\tau = \tau\sigma^{n-1}$ tells us that

$$(\sigma^a\tau^b)(\sigma^{a'}\tau^{b'}) = \sigma^a(\sigma^{(-1)^b a'}\tau^b)\tau^{b'} = \sigma^{a+(-1)^b a'}\tau^{b+b'}.$$

So every element of D_{2n} has a representation as $\sigma^a\tau^b$ for some $a, b \in \mathbb{Z}$. Moreover, the relations $\sigma^n = \tau^2 = e$ mean we can assume $0 \leq a < n$ and $0 \leq b < 2$. Distinct choices of a and b give distinct elements of D_{2n}, so the order of D_{2n} is $2n$.

□

(b) Let n be an odd positive integer, Let D_{4n} be the group generated by the matrices

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix}$$

where ζ is a primitive n-th root of unity. Show that D_{4n} has order $4n$, and give the commutation relations between the above generators.

Denote by τ the first matrix and σ the second matrix. A computation shows that $o(\tau) = 4$ and $o(\sigma) = n$, giving us the relations $\sigma^n = \tau^4 = e$. Another computation gives us the commutation relation $\sigma\tau = \tau\sigma^{n-1}$. This means that we have the group presentation

$$D_{4n} = \langle \sigma, \tau \mid \sigma^n = \tau^4 = e, \sigma\tau = \tau\sigma^{n-1} \rangle.$$

Then, each element of D_{4n} has a representation as $\sigma^a\tau^b$ with $0 \leq a < n$ and $0 \leq b < 4$. Distinct choices of a and b give distinct elements of D_{4n}, so the order of D_{4n} is $4n$.

2 Exercise I.42 Viewing $\mathbb{Z}$, $\mathbb{Q}$ as additive groups, show that $\mathbb{Q}/\mathbb{Z}$ is a torsion group, which has one and only one subgroup of order n for each integer $n \geq 1$, and that this subgroup is cyclic.

Proof. First, note that each element of $\mathbb{Q}/\mathbb{Z}$ has a representative $a/b \in \mathbb{Q}$ such that $a, b \in \mathbb{Z}$ are coprime, $b \geq 1$, and $0 \leq a < b$. Let $a/b \in \mathbb{Q}$; automatically, we may assume that $a, b \in \mathbb{Z}$ are coprime and $b \geq 1$, as all elements of $\mathbb{Q}$ have such a representation. If it is not already the case that $0 \leq a < b$, write $a = kb + a'$ for some $k, a' \in \mathbb{Z}$ with $0 \leq a' < b$. In which case, $\overline{a/b} = \overline{a'/b} \in \mathbb{Q}/\mathbb{Z}$, which is the desired representation.

If $x \in \mathbb{Q}/\mathbb{Z}$ with representative $a/b \in \mathbb{Q}$, as described, then $bx = \overline{a} = 0 \in \mathbb{Q}/Z$, so $o(x) \leq b < \infty$. In particular, $\mathbb{Q}/\mathbb{Z}$ is a torsion group. Moreover, $kx = 0$ if and only if $b \mid ka$, implying that $o(x) = \operatorname{lcm}(a, b)/a$. Since a and b are coprime, $\operatorname{lcm}(a, b) = ab$, so $o(x) = b$.

From this, we deduce that each $x \in \mathbb{Q}/\mathbb{Z}$ has a representative $a/o(x) \in \mathbb{Q}$ with $a, o(x) \in \mathbb{Z}$ coprime and $0 \leq a < o(x)$. It can then be seen that such a representative is unique. If $n = o(x)$ and $0 \leq a, b < n$ such that $\overline{a/n} = \overline{b/n} \in \mathbb{Q}/\mathbb{Z}$, then we must have $a = kn + b$ for some $k \in \mathbb{Z}$. But only $k = 0$ is possibly, implying $a = b$.

For each integer $n \geq 1$, we define a map $\varphi_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $a \mapsto \overline{a/n}$. This map is well-defined and injective since $a \equiv b \pmod{n}$ if and only if $a = kn + b$ for some $k \in \mathbb{Z}$, which is equivalent to $\overline{a/n} = \overline{b/n} \in \mathbb{Q}/\mathbb{Z}$. Moreover, φ_n is a group homomorphism since

$$\varphi_n(a + b) = \overline{(a + b)/n} = \overline{a/n} + \overline{b/n} = \varphi_n(a) + \varphi_n(b).$$

Hence, φ_n is a monomorphism with $\mathbb{Z}/n\mathbb{Z} \cong \operatorname{im} \varphi_n \leq \mathbb{Q}/\mathbb{Z}$. We claim that $H_n = \operatorname{im} \varphi_n$ is the unique subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n.

Now, if $x \in \mathbb{Q}/\mathbb{Z}$ with order n, we know x has a unique representative $a/n \in \mathbb{Q}$ with $0 \leq a < n$. In which case, $x = \varphi_n(a) \in H_n$. This means that H_n contains every element of order n in $\mathbb{Q}/\mathbb{Z}$, so H_n is the unique cyclic subgroup of order n.

Let $H \leq \mathbb{Q}/\mathbb{Z}$ be a finite subgroup; we will prove that $H = H_n$ for some n. If $x \in H$ with order m and unique representative $a/m \in \mathbb{Q}$, there are some $k, h \in \mathbb{Z}$ such that $ka + hm = 1$, then $\overline{1/m} = kx \in H$. In other words, $\overline{1/m} \in H$ if and only if H contains an order m element.

Let n be the maximum positive integer such that $\overline{1/n} \in H$ (which exists since H is finite). Assume, for contradiction, that $\overline{1/m} \in H$ but m does not divide n. Define $g = \gcd(n, m) < m \leq n$, then $n = ag$ and $m = b$ for some $a, b > 1$. Moreover, are some $c, d \in \mathbb{Z}$ such that $cn + dm = g$, so H contains the element

$$\overline{a/n} + \overline{b/m} = \overline{g/nm} = \overline{1/nb}.$$

But $nb > n$, which contradicts the definition of n. Hence, the order of every element of H divides n. Therefore, if $x \in H$ has representative $a/o(x) \in \mathbb{Q}$, we know that $n = bo(x)$ for some $b \in \mathbb{Z}$, then $x = \overline{ab/n} \in H_n$. This shows that $H \leq H_n$. Since we also have $\overline{1/n} \in H$, so $H_n = \langle \overline{1/n} \rangle \leq H$, we conclude that $H = H_n$.

□

3 Exercise I.43 Let H be a subgroup of finite abelian group G. Show that G has a subgroup that is isomorphic to G/H.

Proof. By Theorem 8.1 in Lang, $G \cong \bigoplus_p G(p)$, where p ranges over all primes. Since H is itself a finite abelian group, we also have $H \cong \bigoplus_p H(p)$. By definition, $H(p) = G(p) \cap H$, which means, in particular, that $H(p) \leq G(p)$. Applying a fact about modules to the special case of abelian groups ($\mathbb{Z}$-modules), we obtain $G/H \cong \bigoplus_p G(p)/H(p)$. If there is a subgroup $K_p \leq G(p)$ isomorphic to $G(p)/H(p)$, for each prime p, we can construct a subgroup $\bigoplus_p K_p \leq G$ isomorphic to G/H. Therefore, it suffices to prove the result when G is a p-group.

Assume H is a subgroup of a finite abelian p-group G. Then we can write both G and H as the direct sum of cyclic p-groups, and I think there is a way to get the components to line up such that the problem again reduces to the case of when G is a cyclic p-group. I could not figure out how to show this.

□

4 Exercise I.44 Let $f : A \to A'$ be a homomorphism of abelian groups. Let B be a subgroup of A. Denote by A^f and A_f the image and kernel of f in A respectively, and similarly for B^f and B_f. Show that $[A : B] = [A^f : B^f][A_f : B_f]$, in the sense that if two of these three indices are finite, so is the third, and the stated equality holds.

(For clarity, we use G/H and $\frac{G}{H}$, interchangeably, to denote the quotient of G by H.)

Proof. First note that

$$B/B_f = B/(B \cap A_f) \cong BA_f/A_f$$

and

$$A_f/B_f = A_f/(A_f \cap B) \cong BA_f/B.$$

Then

$$\frac{A^f}{B^f} \cong \frac{A/A_f}{B/B_f} \cong \frac{A/A_f}{BA_f/A_f} \cong \frac{A}{BA_f} \cong \frac{A/B}{BA_f/B} \cong \frac{A/B}{A_f/B_f},$$

so

$$[A : B] = [A/B : 1] = [A/B : A_f/B_f][A_f/B_f : 1] = [A^f : B^f][A_f : B_f],$$

where the second equality holds in the desired sense.

□