Homework 8

43. Let G be a simple group of order 168. Then the number of 7-sylow subgroups, n_7, is equal to 1 mod 7, and divides 24. Then we must have $n_7 = 1, 8$. But G is simple, so we cannot have $n_7 = 1$. Then $n_7 = 8$. Since a group of order 7 is cyclic, each 7-sylow subgroup is generated by each of its non-identity elements. Then the 8 subgroups must have trivial intersection. They each contain 6 elements of order 7, and G can have no other elements of order 7 as they would generate other 7-sylow subgroups. Then G has 48 elements of order 7.

44. (a.) Let $\mathbb{Q}$ be the additive group of the rational numbers. Suppose there is a basis B such that every element of $\mathbb{Q}$ is a unique finite sum of elements of B. Take some $a \in B$. Then we can write

$$\frac{a}{2} = \sum_1^n a_i b_i$$

for $a_i \in \mathbb{Z}$ and $b_i \in B$. But then

$$\sum_1^n 2a_i b_i = a,$$

which is only possible if some $b_j = a$ and $b_i = 0$ for $i \neq j$, and if $2a_i = 1$. But this is a contradiction as $\frac{1}{2} \notin \mathbb{Z}$.

(b.) Let G be the group of nonzero rational numbers under multiplication. I claim that G has a basis given by the set of prime numbers. Choose any $a \in G$. We can uniquely write

$$a = \frac{p_1^{a_1} \cdots p_n^{a_n}}{q_1^{b_1} \cdots q_m^{b_m}} = p_1^{a_1} \cdots p_n^{a_n} \cdot q_1^{-b_1} \cdots q_m^{-b_m},$$

which is a countable product for any $a \in G$. Our basis is a countable and thus G is a free group with countable rank.

45. The element $1/n \in \mathbb{Q}/\mathbb{Z}$ generates a subgroup of order n.

Moreover, let A be a subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n. Then we have $nx = 0$ for any $x \in A$, and thus $nx = m$ for some $m \in \mathbb{Z}$. Then $x = \frac{m}{n}$ for some $0 \leq m < n$. But there are n distinct elements in A, so in fact $A = \{\frac{m}{n} : 0 \leq m < n\}$ and A is cyclic and generated by $\frac{1}{n}$.

Then $\langle \frac{1}{n} \rangle$ is the unique subgroup of order n in $\mathbb{Q}/\mathbb{Z}$.

46. Let $\mathbb{C}^x$ be the group of nonzero complex number under multiplication, and let $\mathbb{T}$ be the subset of unit complex numbers.

Suppose $x \in \mathbb{T}_{tor}$. We can write $x = e^{ia\pi}$ for some $a \in \mathbb{R}$, and thus

$$x^n = e^{ina\pi} = 1 = e^0.$$

Then we have $na = 2m\pi$ for some $m \in \mathbb{Z}$, and thus a is the product of a rational number with 2π.

Moreover, for every $\frac{p}{q} \in \mathbb{Q}$, the element $e^{\frac{2p}{q} i\pi}$ is q-torsion, so that the set of torsion elements is exactly the set $\{e^{2si\pi} : s \in \mathbb{Q}\} \subset \mathbb{T}$.

47. First we show that $\mathbb{Q}/\mathbb{Z}$ is divisible. For any nonzero $x \in \mathbb{Q}/\mathbb{Z}$, we have $x = \frac{p}{q}$ for $0 < q$ and $0 < p < q$. Then let $y = \frac{p}{nq}$ so that $ny = x$, and clearly $y \in \mathbb{Q}/\mathbb{Z}$ since $0 < q$ and $0 < p < q$ implies $0 < nq$ and $0 < p < nq$.

Now we show that if A is an abelian group with subgroup B, and $\varphi : B \to \mathbb{Q}/\mathbb{Z}$ is a homomorphism, then there is an extension $\psi : A \to \mathbb{Q}/\mathbb{Z}$ such that φ is the restriction of ψ to B.

First define a set $B' = \{x \in A : nx \in B \text{ for some } n\}$. We can extend φ to a map φ' on B' using divisibility of $\mathbb{Q}/\mathbb{Z}$, and clearly $B \subset B'$. For each $x \in B'$, let n_x be the smallest positive natural number such that $n_x x \in B$. If $x \in B$, then $n_x = 1$. For numbers in $\mathbb{Q}/\mathbb{Z}$, we need to define what it means to divide by a positive integer. For $\frac{p}{q} \in \mathbb{Q}/\mathbb{Z}$ with $p < q$ and a positive integer n, say

$$\frac{\frac{p}{q}}{n} := \frac{p}{nq}.$$

Also for $p/q, r/q \in \mathbb{Q}/\mathbb{Z}$, we have

$$\frac{p/q}{s} + \frac{r/q}{s} = \frac{p}{sq} + \frac{r}{sq} = \frac{p+r}{qs} = \frac{(p+r)/q}{s}$$

so that the operation is well defined.

Then for any $x \in B'$, let

$$\varphi'(x) := \frac{\varphi(n_x x)}{n_x}$$

using the above definition for division by n_x. Since n_x is unique for each x, the map φ' is well defined. We see that $\varphi(nx) = n\varphi(x)$, so we just need to show additivity.

First note that if $nx \in B$, then n_x must divide n. Suppose here that $n = an_x + b$ for some $b < n_x$. Then $(an_x + b)(x) = (an_x)(x) + b(x) \in B$ and thus $b(x) \in B$ since $(an_x)(x) \in B$. But this is a contradiction since $b < n_x$.

Now choose $x, y \in B'$. Letting $a = \text{lcm}(n_x, n_y)$, we clearly have $a(x+y) \in B$, and thus $kn_{x+y} = a$ for some k. We have

$$\varphi'(x+y) = \frac{\varphi(n_{x+y}(x+y))}{n_{x+y}} = \frac{\varphi(kn_{x+y}x + kn_{x+y}y)}{kx_{x+y}} = \frac{\varphi(ax)}{kn_{x+y}} + \frac{\varphi(ay)}{kn_{x+y}} = \varphi'(x) + \varphi'(y),$$

since by $a = pn_x$ for some p,

$$\frac{\varphi(ax)}{kn_{x+y}} = \frac{b\varphi(n_x x)}{kn_{x+y}} = \frac{a\varphi(x)}{k} = \varphi'(x),$$

and similar for $\varphi(ay)$.

Unless $B' = B$, we have extended the domain of φ. If $B = B'$, we can extend to $B \oplus \mathbb{Z}x$ for some $x \notin B$ by defining $\varphi'(b + nx) = \varphi(b)$ where $b \in B$. It is clear that this is a homomorphism on this direct sum, and that $B \cup \mathbb{Z}x$ really is a direct sum. In either case, we have some extension of φ.

We can order the set of extensions of φ by considering them as subsets of $A \times \mathbb{Q}/\mathbb{Z}$ and ordering by inclusion. We have already shown this set is nonempty, and the union of a chain is an upper bound. Then by Zorn's lemma, there is a maximal extension of φ, name it $\tilde{\varphi}$.

Suppose $X := \text{dom}(\tilde{\varphi})$ is not all of A. Then it is clear from above how we can further extend $\tilde{\varphi}$ to include some $x \in A \setminus X$, either if $nx \in X$ for some n, or if $\{nx : n \in \mathbb{Z}\} \cap X = 0$, contradicting the maximality of $\tilde{\varphi}$. Then the domain of $\tilde{\varphi}$ is A.

The extension is not unique since in order to define $\varphi'(x)$ for $nx \in B$, we had to make an arbitrary decision of which element should be the solution to $\varphi(nx) = ny$.

48. Let G be a finite abelian p-group. We claim that G is generated by its elements of maximal order. Let P be the set of elements of maximal order, say p^n, and let $a \notin P$ be some element of order p^r, $r < n$. Then for any $r \leq s < n$, suppose that

$$p^s(a - b) = 0.$$

Then we have $p^s(a) = 0 = p^s b$, contradicting the order of b. Then $(a - b)$ is order p^n as well, and thus $a = (a - b) + b$, showing that any element of G is a sum of elements of maximal order.

49. (a.) Let p be a prime. We want to find the number of subgroups of order p in $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Any such subgroup will be cyclic.

We can generate some by the elements $(1, a)$ for $0 \leq a < p$. These subgroups intersect trivially, since if $n(1, a) = m(1, b)$ for $0 < m, n < p$, then $(n, na) = (m, mb)$, and thus $n = m$ and $a = b$.

Another subgroup is generated by $(0, 1)$, which is distinct from the subgroups above which do not have 0 in their first coordinate except in the identity element.

Finally, there are $p - 1$ distinct elements of order p in each of the $p + 1$ subgroups, which together with the identity give p^2 elements total. Then there can be no other subgroups of order p, so we have listed all $p + 1$ of them.

(b.) We want to find the number of cyclic subgroups with order p^2 in $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$. We can list p^2 of them, with generators $(1, a)$ for $0 \leq a < p^2$. More can be generated by $(np, 1)$ for $0 \leq n < p$.

We know each subgroup has $p(p - 1)$ generators, and distinct subgroups cannot share generators. So far we have listed $p^2 + p = p(p+1)$ subgroups, each with $p(p-1)$ distinct elements of order p^2. This gives $p^2(p^2 - 1)$ elements of order p^2. But $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$ has exactly this many elements of order p^2, so there can be no other subgroups and we have listed all $p^2 + p$ of them.

(c.) Let $G = \mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ be a group and let $H \simeq \mathbb{Z}_{p^2}$ be a subgroup. Then we know G/H will have order p^3, and will be isomorphic to either $\mathbb{Z}_{p^3}, \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$, or $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

The first option is possible when we take $H = \langle (0, 1) \rangle$.

The second option occurs when $H = \langle (p, 0) \rangle$.

The last option is not possible. G is generated by two elements, while $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ is generated by three. Then there cannot be a surjective homomorphism $G \to \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

50. Let p be a prime. The tate group $T_p(\mathbb{Q}/\mathbb{Z})$ has elements given by sequences

$$x = (x_0, x_1, x_2, \dots),$$

where $x_{n-1} = px_n$, and $x_i \in p^{-i}\mathbb{Z}/\mathbb{Z}$.

If x has at least one x_i nonzero, all x_j must be nonzero for $j \leq i$. Then say x_i has order p^r. if $p^s(x_{i+1}) = 0$, this implies $p^{s-1}x_i = 0$, which is a contradiction unless $s - 1 \geq r$. So the orders of elements increase by p at each step. Then it is impossible for x to have finite order unless all of its elements are zero.

The group $\mathbb{Q}/\mathbb{Z}$ can be embedded into $\mathbb{T}$ by $\frac{p}{q} \mapsto e^{\frac{2ip}{q}\pi}$. No other points in $\mathbb{T}$ are torsion. Then $T_p(\mathbb{Q}/\mathbb{Z})$ is isomorphic to $T_p(\mathbb{T})$.

$T_p(\mathbb{C}^\times)$ is also isomorphic to $T_p(\mathbb{T})$ since all of the torsion elements must lie in the unit circle.