This assignment is due **Tuesday, 28 April, 2020 at 8am on Canvas**. Please write your name, section number, and the names of any collaborators at the top of your homework. Homework should be written or typed legibly using complete sentences. Remember to justify all answers fully!

Problem 1. Prove that if N_1, N_2 are normal subgroups, then

$$N_1N_2 = \{a \cdot b : a \in N_1, b \in N_2\}$$

is a subgroup. Make sure you check it's closed under multiplication *and* inverses. Then verify that $N_1N_2 = N_2N_1$. Hint: because $gN = Ng$ for normal subgroups and any $g \in G$, you can rewrite $g \cdot n$ as $n' \cdot g$ for some other $n' \in N$. This lets you 'commute' N_1 and N_2.

Solution 1. Suppose $N_1, N_2 \trianglelefteq G$. Since N_1 and N_2 are both subgroups, $e_G \in N_1$ and $e_G \in N_2$. Therefore, by definition, $e_G = e_Ge_G \in N_1N_2$. Next we will show N_1N_2 is closed under multiplication. Let $a_1, a_2 \in N_1$ and $b_1, b_2 \in N_2$. Our goal is to show that $a_1b_1a_2b_2 \in N_1N_2$. Since N_1 is normal, $b_1a_2b_1^{-1} \in N_1$. We have

$$\begin{aligned} a_1b_1a_2b_2 &= a_1b_1a_2(b_1^{-1}b_1)b_2 \\ &= (a_1(b_1a_2b_1^{-1}))(b_1b_2) \end{aligned}$$

Since a_1 and $b_1a_2b_1^{-1}$ are in N_1, so is their product $a_1(b_1a_2b_1^{-1})$; and $b_1b_2 \in N_2$. Thus $a_1(b_1a_2b_1^{-1})b_1b_2 \in N_1N_2$, so N_1N_2 is closed under multiplication. Next, we need to show N_1N_2 is closed under inverses. The inverse of ab is $b^{-1}a^{-1}$. Since N_1 is normal, $b^{-1}a^{-1}b \in N_1$. Then

$$\begin{aligned} b^{-1}a^{-1} &= b^{-1}a^{-1}(bb^{-1}) \\ &= (b^{-1}a^{-1}b)b^{-1}, \end{aligned}$$

and since $b^{-1}a^{-1}b \in N_1$ and $b^{-1} \in N_2$, their product $b^{-1}a^{-1} = (b^{-1}a^{-1}b)b^{-1} \in N_1N_2$. We remark that the argument up to this point only required that N_1 be normal; N_2 could have been any subgroup.

It remains to show that $N_1N_2 = N_2N_1$. We make use of the fact that, for any group H, the inversion map $H \ni g \mapsto g^{-1}$ is a bijection from H to itself. Let $a \in N_1$ and $b \in N_2$. Since $(ab)^{-1} = b^{-1}a^{-1}$, and $b^{-1} \in N_2$, $a^{-1} \in N_1$, we see that the inversion map on N_1N_2 maps to N_2N_1. Thus $N_1N_2 \subset N_2N_1$. By symmetry the inversion map on N_2N_1 maps to N_1N_2, proving $N_2N_1 \subset N_1N_2$. Therefore these two groups are equal.

Problem 2. Let $N_1, N_2 \lhd G$ be two normal subgroups. Prove the lemma that I left as an exercise from lecture: if $N_1 N_2 = G$ and $N_1 \cap N_2 = \{e\}$, then every $g \in G$ can be *uniquely* written as $g = n_1 \cdot n_2$ with $n_1 \in N_1$, $n_2 \in N_2$.

Solution 2. We first show that e_G can be written uniquely as a product of an element of N_1 with an element of N_2. Suppose we have written $e_G = n_1 n_2$. Then $n_2 = n_1^{-1}$, so $n_2 \in N_1$. But then $n_2 \in N_1 \cap N_2$, so $n_2 = e_G$, and it follows that $n_1 = e_G$. Thus the unique way of writing e_G as a product of an element from N_1 and an element from N_2 is $e_G e_G$. Now let $g \in G$ be general, and suppose $n_1 n_2 = n_1' n_2' = g$ are two distinct ways of writing g as a product of an element of N_1 and an element of N_2. Then we can write e_G as follows:

$$\begin{aligned} e_G &= gg^{-1} \\ &= n_1 n_2 n_2'^{-1} n_1'^{-1} \\ &= n_1 (n_1'^{-1} n_1') n_2 n_2'^{-1} n_1'^{-1} \\ &= (n_1 n_1'^{-1})(n_1' n_2 n_2'^{-1} n_1'^{-1}). \end{aligned}$$

Then $n_1 n_1'^{-1} \in N_1$ and, since N_2 is normal, $n_1' n_2 n_2'^{-1} n_1'^{-1} \in N_2$, so we've written e_G as a product of an element from N_1 and an element from N_2. Thus $n_1 n_1'^{-1} = e_G = n_1' n_2 n_2'^{-1} n_1'^{-1}$. Since $e_G = n_1 n_1'^{-1}$, we have $n_1'^{-1} = n_1^{-1}$, so $n_1 = n_1'$. Then

$$\begin{aligned} n_1^{-1} g &= n_1^{-1} n_1 n_2 = n_2 \\ &= n_1^{-1} n_1 n_2' = n_2', \end{aligned}$$

so $n_2 = n_2'$ as well. We've thus shown g can be written in a unique way as a product of an element from N_1 and an element from N_2. We remark that we only needed N_2 to be normal for our proof.[1]

Problem 3. Using Theorem 9.3, prove the following isomorphisms:

(a) $\mathbb{R}^\times \cong \mathbb{R}^{>0} \times C_2$, where we think of $C_2 = \{\pm 1\}$ as a subgroup of $\mathbb{R}^\times$.

(b) $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4$. Hint: first find the appropriate subgroups isomorphic to C_2 and C_4.

Solution 3. (a) To apply Theorem 9.3, we need to confirm the following conditions: $\mathbb{R}^{>0} \trianglelefteq \mathbb{R}^\times$, $C_2 \trianglelefteq \mathbb{R}^\times$, $\mathbb{R}^\times = \mathbb{R}^{>0} C_2$, and $\mathbb{R}^{>0} \cap C_2 = \{e\}$. Since $\mathbb{R}^\times$ is

[1] More is true: we only needed N_2 to normalize N_1, i.e. $N_2 \subset \{g \in G : gN_1 g^{-1} = N_1\}$.

abelian, all its subgroups are normal, so the statements $\mathbb{R}^{>0} \trianglelefteq \mathbb{R}^\times$ and $C_2 \trianglelefteq \mathbb{R}^\times$ are automatic. If $s \in \mathbb{R}^\times$, then we can write $s = \operatorname{sgn}(s)|s|$, where

$$\operatorname{sgn} := \begin{cases} 1 \text{ if } s > 0 \\ -1 \text{ if } s < 0. \end{cases}$$

(We can't have $s = 0$, since $\mathbb{R}^\times$ is the set of *nonzero* real numbers.) Since $\operatorname{sgn}(s) \in C_2$ and $|s| \in \mathbb{R}^{>0}$, we've shown that $\mathbb{R}^\times = \mathbb{R}^{>0}C_2$. As for $\mathbb{R}^{>0} \cap C_2$, the only positive number in $C_2 = \{1, -1\}$ is 1, and $1 = e$ is the multiplicative identity of $\mathbb{R}^\times$. Therefore, by Theorem 9.3, $\mathbb{R}^\times = \mathbb{R}^{>0} \times C_2$.

(b) The elements of $(\mathbb{Z}/16\mathbb{Z})^\times$ are the odd numbers 1,3,5,...,15, mod 16. Since $15 \cong -1$ mod 16, and $(-1)^2 = 1$, we know that the subgroup $\langle 15 \rangle \trianglelefteq (\mathbb{Z}/16\mathbb{Z})^\times$ is isomorphic to C_2. Checking the powers of 3 mod 16 reveals

$$\begin{aligned} 3^1 &\equiv 3 & 3^2 &\equiv 9 \\ 3^3 &\equiv 11 & 3^4 &\equiv 1, \end{aligned}$$

so that $\langle 3 \rangle \trianglelefteq (\mathbb{Z}/16\mathbb{Z})^\times$ is isomorphic to C_4. As with part (a) of this problem, we know *every* subgroup of $(\mathbb{Z}/16\mathbb{Z})^\times$ is normal. The next condition of Theorem 9.3 for us to check is that $(\mathbb{Z}/16\mathbb{Z})^\times = \langle 3 \rangle \langle 15 \rangle$. A complete table of the odd residue classes mod 16, expressed as products of elements in $\langle 3 \rangle$ with elements in $\langle 15 \rangle$, suffices to verify this condition.

$$\begin{aligned} 1 &\equiv 1 \cdot 1 & 3 &\equiv 3 \cdot 1 \\ 5 &\equiv 3^3 \cdot 15 & 7 &\equiv 3^2 \cdot 15 \\ 9 &\equiv 3^2 \cdot 1 & 11 &\equiv 3^3 \cdot 1 \\ 13 &\equiv 3 \cdot 15 & 15 &\equiv 1 \cdot 15. \end{aligned}$$

When building this table, it helped to remember that 15 behaves as -1 in $(\mathbb{Z}/16\mathbb{Z})^\times$. The last condition of Theorem 9.3 that we need to verify is that $C_2 \cap C_4 = \langle 15 \rangle \cap \langle 3 \rangle = \{e\}$. Here, $e = 1$ mod 16. We have

$$\begin{aligned} \langle 15 \rangle \cap \langle 3 \rangle &= \{1, 15\} \cap \{1, 3, 9, 11\} \\ &= \{1\}. \end{aligned}$$

Having checked all the conditions of Theorem 9.3, we may conclude that $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4$.

Problem 4. Prove by example that if $H, K < G$ are two non-normal subgroups, then HK is not[2] a subgroup and $HK \neq KH$. Hint: $G = S_3$ was the example I started in lecture.

Solution 4. Consider $G = S_3$, with subgroups $H = \langle (12) \rangle$, and $K = \langle (13) \rangle$. Then

$$HK = \{e, (13), (12), (132)\},$$

while

$$KH = \{e, (13), (12), (123)\}.$$

Furthermore, neither of the subsets HK, KH, of G are subgroups, since they're not closed under inverses: $(132)^{-1} = (123) \notin HK$, and $(123)^{-1} = (132) \notin KH$.

Problem 5. Verify that the set $A[p^\infty] = \{a \in A : |a| = p^k \text{ for some } k \in \mathbb{N}\}$ is a subgroup for any abelian group A.

Solution 5. We treat A as an additive group $(A, +)$ with identity 0. For $n \in \mathbb{N}$ and $a \in A$, we write na to denote $a + a + ... + a$ (added to itself n times). First, $A[p^\infty]$ contains the identity element 0 of A, which always has order $1 = p^0$. Next, suppose α and β are elements of $A[p^\infty]$, with

$$p^a \alpha = 0 = p^b \beta.$$

Then

$$\begin{aligned} p^{a+b}(\alpha + \beta) &= p^{a+b}\alpha + p^{a+b}\beta \\ &= p^b(p^a\alpha) + p^a(p^b\beta) \\ &= p^b(0) + p^a(0) \\ &= 0. \end{aligned}$$

Therefore, the order of $\alpha + \beta$ divides p^{a+b}, and thus is a power of p. Now, $n\alpha = 0$ if and only if $n(-\alpha) = 0$. Therefore, *if* the order of α is a power of p, *then* the order of $-\alpha$ is (the same) power of p, so $A[p^\infty]$ is closed under inverses. Since $A[p^\infty]$ satisfies all the above criteria, it's a subgroup of A.

[2](HK *may* be not a subgroup; on the other hand, it may be. For example, H could be any non-normal subgroup of G, and K a subgroup of H which is also non-normal in G. In that case, $HK = H < G$.)

Problem 6. Prove the following statement: let $a \in A$ is an element of order n in an abelian group A, and let $p_1, \dots, p_r$ be the prime divisors of n. Then we can write

$$a = a_1 + \cdots + a_r$$

where $a_i \in A[p_i^\infty]$, i.e. a_i has p_i-power order.

(a) Prove the base case $r = 1$.

(b) Assume that we have proven the case $r - 1$. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and let $m = p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Verify that $\gcd(p_1^{\alpha_1}, m) = 1$.

(c) As such, we can write $1 = um + vp_1^{\alpha_1}$ for some $u, v \in \mathbb{Z}$. Therefore we know that
$$a = (um + vp_1^{\alpha_1}) \cdot a = um \cdot a + vp_1^{\alpha_1} \cdot a$$
Verify that the $vp_1^{\alpha_1} \cdot a$ has order dividing m and $um \cdot a$ has order dividing $p_1^{\alpha_1}$.

(d) Conclude that the inductive hypothesis applies to $vp_1^{\alpha_1} \cdot a$ and the base case applies to $um \cdot a$, which put together finishes the argument.

This proof is §9.1 if you get stuck.

Solution 6. (See §9.1)

Problem 7. Consider the subset A_p of $\mathbb{Q}/\mathbb{Z}$ that is comprised of all fractions with p-power demoninator, that is,

$$A_p = \left\{ \frac{a}{p^n} + \mathbb{Z} : n \geq 1 \right\}$$

Prove that A_p is an infinite p-group.

Solution 7. First, here is a proof that A_p is infinite. The set

$$\left\{ \frac{1}{p} + \mathbb{Z}, \frac{1}{p^2} + \mathbb{Z}, \frac{1}{p^3} + \mathbb{Z}, ... \right\} \subset A_p$$

is infinite because it admits an injection from the positive integers,

$$\begin{aligned} \mathbb{N} &\hookrightarrow A_p \\ n &\mapsto \frac{1}{p^n}. \end{aligned}$$

This map is injective: if

$$\frac{1}{p^n} - \frac{1}{p^m} \in \mathbb{Z},$$

then, since $\frac{1}{p^n}, \frac{1}{p^m} \in (0, 1]$, we in fact have

$$\frac{1}{p^n} - \frac{1}{p^m} = 0.$$

We can combine the fractions to get $\frac{1}{p^n} - \frac{1}{p^m} = \frac{p^m - p^n}{p^{n+m}} = \frac{0}{p^{n+m}}$, which implies $p^m = p^n$, so $n = m$.
Next, we show that A_p is a p-group, i.e. that the order of every element in A_p is a power of p. In an additive group G, for all $\alpha \in G$, if

$$n\alpha = 0,$$

then $|\alpha|$ divides n. Let $(\frac{a}{p^n} + \mathbb{Z}) \in A_p$. Then

$$\begin{aligned} p^n \left(\frac{a}{p^n} + \mathbb{Z} \right) &= a + \mathbb{Z} \\ &= 0 + \mathbb{Z}. \end{aligned}$$

Therefore, the order of $(\frac{a}{p^n} + \mathbb{Z})$ divides p^n, and thus the order of $\frac{a}{p^n} + \mathbb{Z}$ is itself a power of p.
It remains to show that A_p is a subgroup of $\mathbb{Q}/\mathbb{Z}$. Since $\frac{1}{p^0} + \mathbb{Z} = 0 + \mathbb{Z} \in A_p$, we know that A_p contains the identity element of $\mathbb{Q}/\mathbb{Z}$. A_p is also closed under addition and additive inverses, since

$$\left(\frac{a}{p^n} + \mathbb{Z} \right) + \left(\frac{b}{p^m} + \mathbb{Z} \right) = \left(\frac{p^m a + p^n b}{p^{n+m}} + \mathbb{Z} \right),$$

and

$$-\left(\frac{a}{p^n} + \mathbb{Z} \right) = \frac{-a}{p^n} + \mathbb{Z}.$$

Problem 8. We will now finish up the proof of the classification of finite abelian groups.

(a) Suppose that $a \in A[p^\infty] \cap A[q^\infty]$ for two different primes p, q. Prove that $a = 0$. Hint: what is its order?

(b) Let $p_1, \ldots, p_r$ denote all the prime divisors of $|A| = n$. Prove that

$$A[p_1^\infty] \oplus \cdots \oplus A[p_r^\infty] \to A, (a_1, \ldots, a_r) \mapsto a_1 + \cdots + a_r$$

is an isomorphism. Hint: you know it is surjective and a group homomorphism from other problems, so just cite the appropriate ones and prove injectivity using (a).

(c) Verify that every finite p-group is a direct sum of cyclic p-groups. Let G be such a group, where $|G| = k \cdot p$ for $k \geq 1$ (we haven't proven this yet but you may use it for free). We proceed by complete induction on k. Prove the base case of $k = 1$.

(d) By the hard theorem, $G \cong \langle a \rangle \oplus K$. Apply the inductive hypothesis.

(e) We can now put everything together to write each $A[p_i^\infty]$ as a direct sum of cyclic p_i-groups. Make this last argument.

Solution 8. (a) Suppose $a \in A_p \cap A_q$ for distinct primes p and q. Following the hint, consider the order of a. By Problem 7, this order is a power of p and also a power of q. By the fundamental theorem of arithmetic, the order of a have a unique prime factorization. Thus if $|a| = p^n = q^m$ for some $n, m \in \mathbb{N}$, it must be the case that $n = m = 0$. Therefore $|a| = 1$; thus $a = 0$.

(b) Call the map of Problem 8 (b) "f". Problem 6 shows that f is surjective. To see that it is a group homomorphism, note that since addition commutes:

$$\begin{aligned} f(a_1, ..., a_r) + f(b_1, ..., b_r) &= (a_1 + ... + a_r) + (b_1 + ... + b_r) \\ &= (a_1 + b_1) + ... + (a_r + b_r) \\ &= f(a_1 + b_1, ..., a_r + b_r). \end{aligned}$$

As for injectivity, suppose that

$$f(a_1, ..., a_r) = 0.$$

We already know that if A is an abelian group and $a, b \in A$, and $|a|$ is relatively prime to $|b|$, then $|a||b| = |a + b|$. A simple inductive argument shows that this fact generalizes to r elements whose orders, $|a_1|, |a_2|, ..., |a_r|$, are pairwise relatively prime. The orders of our elements $a_1, ..., a_r$ are pairwise relatively prime because each $|a_j|$ is a power of a unique prime p_j. Therefore,

$$|a_1 + \cdots + a_r| = |a_1||a_2|...|a_r|.$$

Since $a_1 + ... + a_r = 0$, we have that

$$|a_1 + \cdots + a_r| = 1.$$

Therefore

$$|a_1||a_2|...|a_r| = 1.$$

Since for each $i \in \{1, ..., r\}$, $|a_i|$ is a positive integer, it follows that each $|a_i|$ must equal 1. But then $a_i = 0$, for $i \in \{1, ..., r\}$. Thus f is injective.

(c) Following the problem's hint, we take for granted that $|G| = kp$ for some $k \geq 1$. Suppose $k = 1$. Then $|G| = p$. The only group of order p, up to isomorphism, is the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Thus, for the base case $k = 1$, every p-group G of order $kp = p$ is a direct sum of cyclic groups.

(d) Now assume that for all $i \in \{1, ..., k-1\}$, every p-group of order ip is a direct sum of cyclic groups. Suppose G is a group of order kp, and a is a non-identity element of G. By the hard theorem, $G \cong \langle a \rangle \oplus K$. Since K is a subgroup of a p-group, K is also a p-group, and

$$|K| = \frac{|G|}{|a|} = ip$$

for some $i \in \{1, ..., k-1\}$. Therefore, by the inductive hypothesis, $K \cong (\mathbb{Z}/p^{t_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{t_\ell}\mathbb{Z})$, with $t_i \in \mathbb{N}$ not-necessarily-distinct.

(e) Letting $|a| = p^{t_0}$,

$$\begin{aligned} G &\cong (\mathbb{Z}/p^{t_0}\mathbb{Z}) \oplus K \\ &\cong (\mathbb{Z}/p^{t_0}\mathbb{Z}) \oplus (\mathbb{Z}/p^{t_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{t_\ell}\mathbb{Z}), \end{aligned}$$

so G is isomorphic to a direct sum of cyclic p-groups. Now, suppose A is a finite abelian group, and $p_1, ..., p_r$ are the primes dividing A. Then, by Problem 8 (b),

$$A \cong A[p_1^\infty] \oplus \cdots \oplus A[p_r^\infty].$$

And, since each $A[p_i^\infty]$ is a finite p_i-group,

$$A[p_i^\infty] \cong (\mathbb{Z}/p_i^{t_{i1}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_i^{t_{i\ell_i}}\mathbb{Z})$$

is a direct sum of cyclic p-groups. Thus

$$A \cong \bigoplus_{\substack{i\in\{1,\ldots,r\} \\ j\in\{1,\ldots,\ell_i\}}} (\mathbb{Z}/p_i^{t_{ij}}\mathbb{Z})$$

is a direct sum of prime-power order cyclic groups.

Problem 9. Apply the classification to the following groups. First decompose them into the respective $A[p^\infty]$, then apply the inductive process. Recall that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

(a) $\mathbb{Z}/24\mathbb{Z}$

(b) $(\mathbb{Z}/24\mathbb{Z})^\times$ Hint: figure out what this group is in additive notation first.

(c) $\mathbb{Z}/70\mathbb{Z}$

Solution 9. (a) The elements of $\mathbb{Z}/24\mathbb{Z}$ of prime power order are:

Element	Order of Element
$3 + 24\mathbb{Z}$	$8 = 2^3$
$6 + 24\mathbb{Z}$	$4 = 2^2$
$8 + 24\mathbb{Z}$	3
$9 + 24\mathbb{Z}$	$9 = 2^3$
$12 + 24\mathbb{Z}$	$2,$

and the negatives of these elements. Therefore,

$$(\mathbb{Z}/24\mathbb{Z})[2^\infty] = 3\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z},$$

and

$$(\mathbb{Z}/24\mathbb{Z})[3^\infty] = 8\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}.$$

Thus

$$\mathbb{Z}/24\mathbb{Z} \cong (3\mathbb{Z}/24\mathbb{Z}) \oplus (8\mathbb{Z}/24\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z}).$$

Alternatively, we could simply factor $24 = 2^3 * 3$ and write $\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ which are both cyclic p-groups.

(b) $(\mathbb{Z}/24\mathbb{Z})^\times$ is a group of order 8, with elements $\{1, 5, 7, 11, 13, 17, 19, 23\}$ (mod 24). Other than $1 + 24\mathbb{Z}$, every element of $(\mathbb{Z}/24\mathbb{Z})^\times$ has order 2. Therefore

$$(\mathbb{Z}/24\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^3.$$

(c) The elements of $\mathbb{Z}/70\mathbb{Z}$ of prime power order are:

Element	Order of Element
$10 + 70\mathbb{Z}$	7
$14 + 70\mathbb{Z}$	5
$20 + 70\mathbb{Z}$	7
$28 + 70\mathbb{Z}$	5
$30 + 70\mathbb{Z}$	7
$35 + 70\mathbb{Z}$	2,

and the negatives of those elements. Therefore

$$\begin{aligned}(\mathbb{Z}/70\mathbb{Z})[2^\infty] &= 35\mathbb{Z}/70\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z},\\ (\mathbb{Z}/70\mathbb{Z})[5^\infty] &= 14\mathbb{Z}/70\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z}, \text{ and}\\ (\mathbb{Z}/70\mathbb{Z})[7^\infty] &= 10\mathbb{Z}/70\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z}.\end{aligned}$$

Thus

$$\mathbb{Z}/70\mathbb{Z} = (35\mathbb{Z}/70\mathbb{Z}) \oplus (14\mathbb{Z}/70\mathbb{Z}) \oplus (10\mathbb{Z}/70\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/5\mathbb{Z}) \oplus (\mathbb{Z}/7\mathbb{Z}).$$

Alternatively, since $70 = 2 * 5 * 7$ we can write $\mathbb{Z}/70\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ which is a direct sum of cyclic p-groups.

Problem 10. The *elementary divisors* of A are exactly those prime powers $p_i^{\alpha_i}$ appearing in the classification:

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

where, again, we allow repeats. This means that $|A| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. The above discussion implies (but does not quite prove) that $A \cong B$ if and only if they have the same elementary divisors. As such, the number of finite abelian groups of an order n depends on the number of ways n can be split up into elementary divisors. For example there are 4 groups of order 36 corresponding to

$$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 4 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 9 = 4 \cdot 9$$

Repeat the same process to determine how many[3] groups of the following orders there are: (a) 12, (b) 30, (c) 72, (d) 144, (e) 600, (f) 1160, (g) p^4 for p a prime.

Solution 10. For $n \in \mathbb{N}$, let $p(n)$ be the number of *integer partitions* of n, i.e. ways of expressing

$$n = \alpha_1 + \alpha_2 + ... + \alpha_\ell$$

with $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_\ell$ all positive integers. We saw integer partitions in Problem 3 of Homework 9, for example. If $n = p_1^{a_1} p_2^{a_2} ... p_m^{a_m}$ with the p_is being distinct primes, then the number of ways n can be split into elementary divisors is $p(a_1)p(a_2)...p(a_m)$.

(a)

$$\begin{aligned} 12 &= 2^2 \cdot 3 \\ &= 2 \cdot 2 \cdot 3 \end{aligned}$$

(b)

$$30 = 2 \cdot 3 \cdot 5.$$

(c)

$$\begin{aligned} 72 &= 2^3 \cdot 3^2 \\ &= 2^3 \cdot 3 \cdot 3 \\ &= 2^2 \cdot 2 \cdot 3^2 \\ &= 2^2 \cdot 2 \cdot 3 \cdot 3 \\ &= 2 \cdot 2 \cdot 2 \cdot 3^2 \\ &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3. \end{aligned}$$

[3](abelian)

(d)

$$\begin{aligned}
144 &= 2^4 \cdot 3^2 \\
&= 2^4 \cdot 3 \cdot 3 \\
&= 2^2 \cdot 2^2 \cdot 3^2 \\
&= 2^2 \cdot 2^2 \cdot 3 \cdot 3 \\
&= 2^3 \cdot 2 \cdot 3^2 \\
&= 2^3 \cdot 2 \cdot 3 \cdot 3 \\
&= 2^2 \cdot 2 \cdot 2 \cdot 3^2 \\
&= 2^2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \\
&= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3^2 \\
&= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3.
\end{aligned}$$

(e)

$$\begin{aligned}
600 &= 2^3 \cdot 3 \cdot 5^2 \\
&= 2^3 \cdot 3 \cdot 5 \cdot 5 \\
&= 2^2 \cdot 2 \cdot 3 \cdot 5^2 \\
&= 2^2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \\
&= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5^2 \\
&= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5.
\end{aligned}$$

(f)

$$\begin{aligned}
1160 &= 2^3 \cdot 5 \cdot 29 \\
&= 2^2 \cdot 2 \cdot 5 \cdot 29 \\
&= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 29.
\end{aligned}$$

(g) For p a prime in general, we have

$$\begin{aligned}
p^4 &= p^4 \\
&= p^2 \cdot p^2 \\
&= p^3 \cdot p \\
&= p^2 \cdot p \cdot p \\
&= p \cdot p \cdot p \cdot p.
\end{aligned}$$

Problem 11. Let A be a finite abelian group with order divisible by p. Prove that A has an element of order p. Hint: prove that there is a cyclic subgroup of p-power order in the direct sum decomposition of A, then prove that every p-power cyclic group has an element of order p.

Solution 11. Let $A \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/p_m^{a_m}\mathbb{Z})$, using the fundamental theorem of finite abelian groups (Problem 8). Then $|A| = p_1^{a_1}p_2^{a_2}...p_m^{a_m}$, so p divides $p_1^{a_1}...p_m^{a_m}$. Therefore p is one of the factors in the elementary divisor decomposition, i.e. $p = p_j$ for some $j \in \{1, ..., m\}$. It suffices then to show that $\mathbb{Z}/p^{a_j}\mathbb{Z}$ has an element of order p, since $\mathbb{Z}/p^{a_j}\mathbb{Z} \trianglelefteq A$. And clearly the element $p^{a_j-1} + p^{a_j}\mathbb{Z}$ has order p, i.e. $p * [p^{a_j-1}] = [p^{a_j}] = [0]$.