1 Spring 2002 – Group Theory

Problem 1.1. Show that a group of order $2m$, where m odd, has a normal subgroup of order m.

Solution: Let G be a group of order $2m$ with m odd. Let G act on itself by left multiplication. This gives

$$\lambda : G \longrightarrow S_{2m}$$

by

$$g \mapsto \lambda_g : x \mapsto g \cdot x.$$

Notice that $ker(\lambda) = \{e\}$ and furthermore λ_g has no fixed point for $g \neq e$: $g \cdot x = x \Rightarrow g = e$. Since $\lambda(G) \cong G$ has order $2m$, Cauchy's Theorem says that there is an element $\lambda_g \in \lambda(G)$ of order 2. Write λ_g as a product of disjoint cycles:

$$\lambda_g = \sigma_1 \dots \sigma_r.$$

Since λ_g has order two, the σ_i are all transpositions. Since λ_g has no fixed point, λ_g moves $2m$ points and hence $r = m$ is odd. Therefore

$$\lambda_g \notin A_{2m} \Rightarrow \lambda(G) \subsetneq A_{2m} \Rightarrow A_{2m}\lambda(G) = S_{2m},$$

since $\frac{|S_{2m}|}{|A_{2m}|} = 2$. Finally by the Second Isomorphism Theorem and the fact that $A_{2m} \lhd S_{2m}$ (Any $\sigma \in A_{2m}$ is a product of an even number of transpositions, so if $\tau \in S_{2m}$, then writing τ as a product of transpositions, it is clear that $\tau\sigma\tau^{-1}$ is a product of an even number of transpositions, hence in A_{2m}), we have

$$\frac{S_{2m}}{A_{2m}} = \frac{A_{2m}\lambda(G)}{A_{2m}} \cong \frac{\lambda(G)}{A_{2m} \cap \lambda(G)},$$

so since λ is an isomorphism, $\exists H \subset G$ a subgroup such that $\lambda(H) = A_{2m} \cap \lambda(G)$ and $[G : H] = 2$ (since $[S_{2m} : A_{2m}] = 2$). We are done since subgroups of index 2 are automatically normal (If $H \subset G$ is a subgroup of index 2, let $G/H = \{H, aH\}$. For any $g \in G \setminus H$, $gH = aH = Hg$ and so $gHg^{-1} = H$). $\square$

- Left Multiplication: G acting on itself by left multiplication is a transitive action with no fixed point for $e \neq g \in G$.
- Cayley's Theorem I: Let G be a group s.t. $|G| = n$, then $G \hookrightarrow S_n$ via

$$\lambda : G \longrightarrow S_n : g \mapsto \lambda_g : x \mapsto g \cdot x.$$

- Cycle Decomposition: $\tau \in S_n$, then $\tau = \sigma_1 \dots \sigma_r$ a product of disjoint cycles (uniquely).
- Transposition Decomposition: $\tau \in S_n$, then $\tau = \gamma_1 \dots \gamma_r$ a product of (not necessarily disjoint) transpositions, where $r \pmod 2$ is unique.
- Alternating Group: $A_n \subset S_n$ group of even permutations (can be written as an even number of transpositions), then $[S_n : A_n] = 2$ and $A_n \lhd S_n$.
- Cauchy's Theorem: $|G| = n$ and p prime s.t. $p \mid n$, then $\exists a \in G$ s.t. $o(a) = p$.
- Second Isomorphism Theorem: If G is a group and A, $B \subset G$ are subgroups s.t. $B \lhd G$, then
$$\frac{AB}{B} \cong \frac{A}{A \cap B}.$$
- Index 2 Subgroups: $[G : H] = 2 \Rightarrow H \lhd G$.

Problem 1.2. List, up to isomorphism, all finite abelian groups A satisfying the following:

(i) A is a quotient of $\mathbb{Z}^2$, and

(ii) A is annihilated by 18, i.e. $18a = e$ for all a in A.

Your list should contain a representative of each isomorphism class exactly once. How many groups are there?

Solution: First note that quotients of $\mathbb{Z}^2$ look like $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (If $H \subset \mathbb{Z}^2$ is a subgroup, then H is finitely generated free of rank 1 or 2. By considering a basis in which the basis of H is $\{u_1 e_1, u_2 e_2\}$ (u_1, u_2 are natural numbers with u_2 possibly 0), where $\{e_1, e_2\}$ is a basis of $\mathbb{Z}^2$, we see that $\mathbb{Z}^2/H \cong \mathbb{Z}/u_1\mathbb{Z} \times \mathbb{Z}/u_2\mathbb{Z}$. If $H = \langle (a, 0) \rangle$, then $\mathbb{Z}^2/H = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}$. This can be visualized as the lattice points of the strip $\{(x, y) \mid 0 \le x < a\}$. Similarly, if $H = \langle (a, 0), (0, b) \rangle$, then $\mathbb{Z}^2/H = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ can be visualized as lattice points of the rectangle $\{(x, y) \mid 0 \le x < a, 0 \le y < b\}$. If $H = \langle (a, b) \rangle$ where $a \ne 0$ and $b \ne 0$, similar geometric descriptions can be made.) For $a = 1$, we must have $b \mid 18$, and we get

$$\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}.$$

For $a > 1$, we must have $a \mid 18$ and $b \mid 18$. Also, by the Fundamental Theorem of Finitely Generated Abelian Groups I, $a \mid b$ (or just note that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ if $n = kl$ and $(k, l) = 1$). This gives us

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z},$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z},$$

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}, \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}.$$

This gives us a total of 16 groups.

Alternatively, we could have just directly applied the Fundamental Theorem of Finitely Generated Abelian Groups I and found all finite abelian groups which has the biggest invariant factor a divisor of 18 and which is at most a direct product of two factors. $\square$

- Quotients of $\mathbb{Z} \times \mathbb{Z}$: Quotients of $\mathbb{Z}^2$ look like $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.
- $\mathbb{Z}/n\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ if $n = kl$ and $(k, l) = 1$.
- Fundamental Theorem of Finitely Generated Abelian Groups I: Finitely generated abelian groups look like
$$\mathbb{Z}/u_1\mathbb{Z} \times \cdots \times \mathbb{Z}/u_m\mathbb{Z} \times \mathbb{Z}^r,$$
where $u_i|u_{i+1}$, $1 \leq i < m$ are uniquely determined.
- Free Abelian Groups: An abelian group can be viewed as a "vector space" over $\mathbb{Z}$ (or (sub)lattice points of the plane).
  - The notions of generating sets, linear independence, basis, and invariance of dimension (called rank) carry over.
  - A finitely generated abelian group is free if it has a basis.
  - Subgroups of free abelian groups of rank n are free of rank $\leq n$.
  - If $\{e_1, \ldots, e_n\}$ is a basis of $\mathbb{R}^n$, the subgroup generated by $\{e_1, \ldots, e_n\}$ is a free abelian group of rank n and correspond to the set of vectors with integer coordinates in the basis.
  - But a free abelian group of rank $n > 0$ can contain subgroups of the same rank that do *not* coincide with the group, e.g. $m\mathbb{Z} \subsetneq \mathbb{Z}$ for $m > 0$ also has rank 1.

Problem 1.3. Prove that a group G of order 120 is not simple.

Solution: Suppose G is simple. $120 = 2^3 \cdot 3 \cdot 5$. By Sylow's Theorem, the number of Sylow 5–subgroups are
$$n_5 = 1 + 5k = 1, 6, 11, \ldots$$
and must divide $2^3 \cdot 3 = 24$. So the only possibilities are $n_5 = 1, 6$. If $n_5 = 1$, then the Sylow 5–subgroup is normal, so it must be the case that $n_5 = 6$. Let G act on the set of Sylow 5–subgroups by conjugation. This induces
$$\lambda : G \longrightarrow S_6 : g \mapsto \lambda_g : P \mapsto gPg^{-1}.$$
Since G is simple, it must be the case that $ker(\lambda) = \{e\}$ or $ker(\lambda) = G$. It cannot be the case that $ker(\lambda) = G$, because by Sylow's Theorem, all Sylow 5–subgroups are conjugate

so G in fact acts transitively. On the other hand, if $ker(\lambda) = \{e\}$, then $G \cong \lambda(G)$ is a subgroup of S_6. Now

$$A_6 \cap \lambda(G) \lhd \lambda(G) \Rightarrow A_6 \cap \lambda(G) = \{e\} \text{ or } \lambda(G).$$

If $A_6 \cap \lambda(G) = \{e\}$, then

$$\frac{|A_6||\lambda(G)|}{|A_6 \cap \lambda(G)|} = |A_6\lambda(G)| > 6!,$$

which is impossible since $A_6\lambda(G) \subset S_6$. So

$$A_6 \cap \lambda(G) = \lambda(G) \Rightarrow \lambda(G) \subsetneq A_6.$$

Now let A_6 act on $A_6/\lambda(G)$ by left multiplication. This induces

$$\gamma : A_6 \longrightarrow S_3 : x \mapsto \gamma_x : y\lambda(G) \mapsto xy\lambda(G).$$

We have that

$$\begin{aligned}
ker(\gamma) &= \{x \mid xy\lambda(G) = y\lambda(G), \forall y \in A_6\} \\
&= \{x \mid y^{-1}xy \in \lambda(G), \forall y \in A_6\} \\
&= \{x \mid x \in y\lambda(G)y^{-1}, \forall y \in A_6\} \\
&= \bigcap_{y \in A_6} y\lambda(G)y^{-1} \\
&\subset \lambda(G),
\end{aligned}$$

so in particular $ker(\lambda) \neq A_6$. On the other hand, the action is transitive so it cannot be the case that $ker(\lambda) = A_6$. We therefore conclude that $\ker(\lambda) \lhd A_6$, which is a contradiction since A_6 is simple. $\square$

- Just Counting: Let G be a group and let A, B be subsets of G. Then

$$|AB| = \frac{|A||B|}{|A \cap B|}.$$

- Cayley's Theorem II: Let G be a group and $H \subset G$ a subgroup. Then G acting on H by left multiplication induces

$$\lambda : G \longrightarrow S_{[G:H]} : g \mapsto \lambda_g : aH \mapsto gaH.$$

  The action is transitive, aH is a fixed point of g if and only if $g \in aHa^{-1}$, hence

$$ker(\lambda) = \bigcap_{a \in G} aHa^{-1}.$$

- Group Action: Let G be a group. Let X be a set. Let G act on X.
  - For $x \in X$, $Gx = \{gx \in X \mid g \in G\} \subset X$ is the orbit of x.
  - For $x \in X$, $G_x = \{g \in G \mid gx = x\} \subset G$ is the stabilizer of x.
  - $X^g = \{x \in X \mid gx = x\}$ is the set of fixed points of g.
  - $X^G = \{x \in X \mid gx = x, \forall g \in G\} \subset X$ is the set of fixed points of G.
  - $X/G = \{Gx \mid x \in X\}$ is the set of orbits of X.
- Size of an Orbit:
  $$|Gx| = [G : G_x].$$
  In fact there is a natural action isomorphism between Gx and G/G_x.
- Orbit Decomposition I: Orbits of X partition X, say have orbits $\{G_{x_1}, \ldots, G_{x_n}\}$, then
  $$|X| = \sum_i |Gx_i|.$$
- Orbit Decompositioni II:
  $$|X| = |X^G| + \sum_k |Gx_k|,$$
  where the sum are now only over orbits of size > 1.
- Burnside's Formula:
  $$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$
- Sylow's Theorem: Let G be a finite group of order $|G| = p^n \cdot m$ s.t. $p \nmid m$.

  (i) Sylow p–subgroups exist.

  (ii) Any p–subgroup of G is contained in some Sylow p–subgroup.

  (iii) All Sylow p–subgroups are conjugate.

  Let n_p denote the number of Sylow p–subgroups. Then

  (iv) $n_p \equiv 1$ modulo p.

  (v) $n_p \mid m$.

  - To prove (i), first show a non–trivial p–group G has non–trivial center by letting G act on 2^G (subgroups of G) by conjugation. Then let G be a general group and act on itself by conjugation and proceed by induction on $|G|$.

- To prove (ii), let $S \subset G$ be a Sylow p–subgroup, S_1 any p–subgroup, and let S_1 act on G/S by left multiplication and observe that S_1 has at least one fixed point.
- To prove (iii), let S, S_1 be Sylow p–subgroups and proceed as above.
- To prove (iv), let S be a Sylow p–subgroup and $C(S)$ the class of subgroups conjugate to S. Let S act on $C(S)$ by conjugation and observe that the only fixed point is S itself.
- To prove (v), let S be a Sylow p–subgroup. Let G act on 2^G by conjugation and observe that $n_p = |G \cdot S| = [G : N_G(S)] \mid m$.

- Simplicity of A_n: A_n is simple for $n \geq 5$.

2 Winter 2002 – Groups

Problem 2.1. Let G be a free abelian group of rank n for a positive integer n (therefore $G \cong \mathbb{Z}^n$ as groups).

(a) Prove for a given integer $m > 1$, there are only finitely many subgroups H of index m in G;

(b) Find a formula of the number of subgroups of G of index 3. Justify your answer.

Solution: (a) If $H \subset G$ is a subgroup of index m. Then G acting on G/H by left multiplication gives

$$\lambda_H : G \longrightarrow S_{[G:H]} = S_m.$$

This in turn gives a map

$$\phi : \{\text{subgroups of } G \text{ of index } m\} \longrightarrow \{G \to S_{[G:H]}\} : H \mapsto \lambda_H$$

The latter set is finite since any $\lambda : G \longrightarrow S_m$ is determined by $\lambda(g_1), \ldots, \lambda(g_n)$, where $G = \langle g_1, \ldots, g_n \rangle$, and hence $|\{G \to S_{[G:H]}\}| \leq (m!)^n$. So it suffices to show that ϕ is one-to-one. For this we observe that

$$ker(\lambda_H) = \bigcap_{g \in G} gHg^{-1} = H,$$

since G is abelian. Therefore if $H \neq H'$ are two subgroups of index m, $ker(\lambda_H) \neq ker(\lambda_{H'})$, which implies that $\lambda_H \neq \lambda_{H'}$.

(b) I screwed up this problem at first, but in any case, consider maps from $\mathbb{Z}^n$ onto $\mathbb{Z}/3\mathbb{Z}$ (where do the generators go?). The kernel of such a map would correspond to a subgroup of index 3.

$\square$

Problem 2.2. Prove or disprove: there exists a finite abelian group G whose automorphism group has order 3.

Solution: This is not true. Let G be a finite abelian group with $Aut(G) \cong \mathbb{Z}/3\mathbb{Z}$. Then

$$\phi : G \longrightarrow G : x \mapsto x^{-1}$$

is an automorphism since G is abelian (so $\phi(xy) = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$). But ϕ clearly has order 2 and since $2 \nmid 3$, it must be the case that $\phi \equiv Id_G$. This implies that $x = x^{-1}$, for all $x \in G$. An application of the Fundamental Theorem of Finitely Generated Abelian Groups gives that $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, some n. Every non–zero element in $(\mathbb{Z}/2\mathbb{Z})^n$ has order 2, and since any automorphism is determined by its action on the the n generators $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$, we see that $|Aut((\mathbb{Z}/2\mathbb{Z})^n)| = (2^n - 1)^n$. Checking $n = 1, 2$, we have a contradiction. □

Problem 2.3. Let S and G be p–groups (with $G \neq \{e\}$), and assume that S acts on G by automorphisms. Show that the fixed subgroup $G^S = \{g \in G \mid s(g) = g, \forall s \in S\}$ is non–trivial (i.e., is not the trivial subgroup $\{e\}$).

Solution: We use the Orbit Decomposition Formula:

$$|G| = |G^S| + \sum_{g_i} |Sg_i|,$$

where the sum is over disjoint orbits of size bigger than 1. Next we note that $|Sg_i| = [S : S_{g_i}]$, where

$$S_{g_i} = \{s \in S \mid sg_i = g_i\}$$

is the stabilizer of g_i. The g_i's are not fixed points of the action by S, so

$$[S : S_{g_i}] = |Sg_i| > 1 \Rightarrow p \mid [S : S_{g_i}]$$

since S is a p-group. Also, $p \mid |G|$ since G is a p-group, so we conclude that $p \mid |G^S|$, which implies that G^S is non–trivial. □

3 Fall 2002 – Group Theory

Problem 3.1. Let A be a free abelian group of rank n. If H is a subgroup of A, show that H is free abelian of rank n if and only if A/H is finite.

Solution: First note that if H is a subgroup of a free abelian group A, then

a) H is free abelian of rank $\leq n$ (This is proved by induction. $n = 0$ is trivial. For $n > 0$, let $\{e_1, \ldots, e_n\}$ be a basis for A and let $A_1 = \langle e_1, \ldots, e_{n-1}\rangle$. This is free abelian of rank $n-1$, so $H_1 = H \cap A_1$ is free abelian of rank $m \leq n-1$ by induction. Let $\{f_1, \ldots, f_m\}$ be a basis for H_1. The last coordinates of elements of H in the basis $\{e_1, \ldots, e_n\}$ form a subgroup of $\mathbb{Z}$ and hence has the form $k\mathbb{Z}$, for some k. If $k = 0$ then we are done. If $k > 0$, then let f_{m+1} be an element of H with last coordinate k. Then $\{f_1, \ldots, f_m, f_{m+1}\}$ is a basis for H) and that

b) there is a basis $\{e_1, \ldots, e_n\}$ of A and natural numbers $u_1, \ldots, u_m$ s.t. $\{u_1e_1, \ldots, u_me_m\}$ is a basis of H (To prove this, let $\{f_1, \ldots, f_m\}$ be a basis of H and $\{e_1, \ldots, e_n\}$ a basis of A. There is an integral $n \times m$ matrix C of rank m such that (*) $(f_1, \ldots, f_m) = (e_1, \ldots, e_n)C$. There is also an inductive procedure (like Smith Normal Form but easier) which turns any integral matrix into a "diagonal" matrix using "elementary" operations. Applying the elementary operations to C and applying the appropriate ones to the basis of H and A will turn C into some $diag(u_1, \ldots, u_m)$ while preserving (*). This gives exactly that $f_i = u_ie_i$).

$\Longleftarrow$: Suppose $H \subset A$ is free abelian of rank n. Let $\{e_1, \ldots, e_n\}$ and $\{u_1, \ldots, u_n\}$ be as in b). Let

$$\phi : A \longrightarrow \mathbb{Z}^n : a \mapsto (a_1, \ldots, a_n),$$

where $(a_1, \ldots, a_n)$ are the coordinates of a in the basis $\{e_1, \ldots, e_n\}$. Under ϕ, we have that

$$A/H \cong \mathbb{Z}^n/(u_1\mathbb{Z} \times \cdots \times u_n\mathbb{Z}) \cong \mathbb{Z}/u_1\mathbb{Z} \times \cdots \times \mathbb{Z}/u_m\mathbb{Z},$$

where the last $\cong$ comes from the fact that in general $(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong A_1/B_1 \times \cdots \times A_n/B_n$, if $B_i \lhd A_i, 1 \leq i \leq n$.

$\Longrightarrow$: Conversely, suppose A/H is finite abelian. H is free abelian by a). Assume towards a contradiction that H is of rank $m < n$. Let $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_m\}$ satisfy the conclusion of b) and let ϕ be as in the previous paragraph, then under ϕ,

$$A/H \cong \mathbb{Z}^n/(u_1\mathbb{Z} \times \cdots \times u_m\mathbb{Z}) \cong (\mathbb{Z}/u_1\mathbb{Z} \times \cdots \times \mathbb{Z}/u_m\mathbb{Z}) \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{(n-m)–times}}.$$

But the group on the right hand side is clearly infinite, a contradiction. □

- Quotient of Direct Product: If $A_1, \ldots, A_n$ are groups, then

$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong A_1/B_1 \times \cdots \times A_n/B_n,$$

  if $B_i \lhd A_i, 1 \leq i \leq n$. In particular this is always true if the A_i's are all abelian.

- Subgroup of Free Abelian Group I: A subgroup of a free abelian group of rank n is free abelian of rank $\leq n$.

- Subgroup of Free Abelian Group II: If A is a free abelian group of rank n and $H \subset A$ is a subgroup, then there is a basis $\{e_1, \ldots, e_n\}$ of A and natural numbers $u_1, \ldots, u_m$ s.t. $\{u_1 e_1, \ldots, u_m e_m\}$ is a basis of H.

Problem 3.2. Let G be a finite group of order 108. Show that G has a normal subgroup of order 9 or 27.

Solution: $108 = 2^2 \cdot 3^3$. By Sylow's Theorem, $n_3 = 1 + 3k = 1, 4, 7, \cdots \mid 2^2$, where n_3 is the number of 3–Sylow subgroups. If $n_3 = 1$, then again by Sylow's Theorem, we know that the unique 3–Sylow subgroup is normal of order $3^3 = 27$. Suppose then that $n_3 = 4$. Let P_1, P_2, P_3, P_4 denote the four 3–Sylow subgroups. Basic counting gives that

$$|P_1 P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = \frac{3^3 \cdot 3^3}{|P_1 \cap P_2|} \leq 3^3 \cdot 2^2.$$

Since $P_1 \neq P_2$, we conclude that $|P_1 \cap P_2| = 3^2$. Similarly $|P_i \cap P_j| = 3^2, \forall i \neq j$. Next let $P \equiv P_1 \cap P_2$ act on $\mathcal{C} = \{P_1, P_2, P_3, P_4\}$ by conjugation. The Orbit Decomposition Formula gives:

$$4 = |P^{\mathcal{C}}| + \sum [P : N_P(P_i)],$$

where $P^{\mathcal{C}}$ denotes the fixed set, the sum is over all orbits of size bigger than one and $N_P(P_i)$ is the subgroup of elements of P which normalizes P_i. Since P is a 3–group, 3 divides each term in the sum. But $P \subset P_1, P_2$ and so we have at least 2 fixed points. This implies that the sum is empty and therefore

$$P \subset N_G(P_3), N_G(P_4).$$

P_3 is normal in $N_G(P_3)$ and hence is the unique 3–Sylow subgroup by Sylow's Theorem. Again by Sylow's Theorem this implies that $P \subset P_3$. Similarly we conclude $P \subset P_4$. This together with the previous counting means that $P_i \cap P_j = P, \forall i, j$ and therefore

$$P = P_1 \cap P_2 = P_1 \cap P_2 \cap P_3 \cap P_4.$$

Finally we notice that

$$gPg^{-1} \subset gP_1g^{-1} \cap gP_2g^{-1} \cap gP_3g^{-1} \cap gP_4g^{-1} = P, \forall g \in G,$$

where the equality follows from the conjugacy part of Sylow's Theorem. So $P \lhd G$ and $|P| = 9$. □

- Normal p–Group: Let G be a group and $p \mid |G|$. If P is the intersection of all p–Sylow subgroups of G, then P is normal.

Problem 3.3. Let G be a finite group and P a p–Sylow subgroup. Let $N_G(P)$ be the normalizer of P in G. Show that:

a) P is the unique p–Sylow subgroup of $N_G(P)$ (Don't quote a theorem that this is true!)

b) $N_G(P)$ is self–normalizing in G.

Solution: a) Suppose Q is a p–Sylow subgroup of $N_G(P)$. Let Q act on $N_G(P)/P$ by left multiplication. The Orbit Decomposition Formula says:

$$[N_G(P) : P] = |Q^{N_G(P)/P}| + \sum Q_{gP},$$

where $Q^{N_G(P)/P}$ denotes the set of fixed points, the sum is over all orbits of size bigger than one and Q_{gP} is the stabilizer of gP. Q is a p–group so p divides each term in the sum, but P is p–Sylow so $p \nmid [N_G(P) : P]$. This implies there is at least one fixed point. So say gP is a fixed point, then

$$(\forall q \in Q)(qgP = gP \Rightarrow g^{-1}qgP = P \Rightarrow q \in gPg^{-1}) \Longrightarrow Q = gPg^{-1},$$

where the last implication follows since $|P| = |Q|$. But $P \lhd N_G(P)$ so $Q = gPg^{-1} = P$.

b) Suppose $N_G(P)$ were not self–normalizing, then $M \equiv N_G(N_G(P)) \supsetneq N_G(P)$ and $P \lhd N_G(P) \lhd M$. Let $g \in M$, then $gPg^{-1} \subset N_G(P)$, hence must be equal to P by a). This implies that $P \lhd M$, which contradicts the fact that $N_G(P)$ is the maximal subgroup of G which normalizes P. $\square$

4 Winter 2003 – Groups

Problem 4.1. List, up to isomorphism, all abelian groups A which satisfy the following three conditions:

(i) A has 108 elements;

(ii) A has an element of order 9;

(iii) A has no element of order 24.

Solution: $108 = 2^2 \cdot 3^3$. If G is an abelian group of order 108, then the Fundamental Theorem of Finitely Generated Abelian Groups II says that

$$G \cong P_2 \times P_3,$$

where P_2 and P_3 are the Sylow 2 and 3 subgroups of G. We have that

$$2 = 0 + 2 = 1 + 1, 3 = 3 + 0 = 1 + 2,$$

so we have the following possibilities:

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \cong \mathbb{Z}/108\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z},$$

where of course the form the groups take on on the right hand side of $\cong$ are the form used in Fundamental Theorem of Finitely Generated Abelian Groups I (To go from one form to the other, we used the fact that if $(k,l) = 1$, then $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}/kl\mathbb{Z}$: Both groups have the same order so it suffices to produce an element in $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ which has order kl, but this is easy, take e.g. (1, 1)). Next we notices that it is impossible for any group of order 108 to have an element of order 24 by Lagrange's Theorem since $24 \nmid 108$. Finally from the form of the groups on the right hand side of $\cong$, it is easy to see that all four groups we have listed satisfy item (ii) (e.g. (0,4) is an element of order 9 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$). □

- Lagrange's Theorem: Let G be a finite group and H its subgroup. Then

$$|G| = [G : H]|H|.$$

  In particular $|H| \mid |G|$ and hence if $x \in G$ $|\langle x \rangle| \mid |G|$ so the order of any element in G must divide $|G|$.

- Fundamental Theorem of Finitely Generated Abelian Groups II: if G is a finite abelian group s.t. $|G| = n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, then

$$G \cong A_1 \times A_2 \times \cdots \times A_m,$$

  where $|A_i| = p^{\alpha_i}$. In addition,

$$A_i \cong \mathbb{Z}/{p_i}^{\beta_{i_1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_i}^{\beta_{i_k}}\mathbb{Z},$$

  where $\beta_{i_1} + \beta_{i_2} + \cdots + \beta_{i_k} = \alpha_i$.

- $\mathbb{Z}/n\mathbb{Z}$: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$ if $n = kl$ and $(k,l) = 1$.

Problem 4.2. Let $N \geq 1$ be a positive integer. Show that a finitely generated group G has only finitely many subgroups of index at most N.

Solution: This follows from the fact that for each integer n there are only finitely many subgroups of index n. Suppose we are given a subgroup $H \subset G$ of index n. Label the cosets of H as $\{a_1H, \ldots, a_nH\}$ such that $a_1 = e$. We let G act on the cosets of H by left multiplication, which induces

$$\lambda_H : G \longrightarrow S_n : g \mapsto \lambda_H(g) : aH \mapsto gaH.$$

G is finitely generated, so say $G = \langle g_1, \ldots, g_m \rangle$. The map λ_H is completely determined by $\{\lambda_H(g_1), \ldots, \lambda_H(g_m)\}$ and hence there are only $(n!)^m$ possible such maps. Hence it suffices to show that if $H \neq H'$ are two subgroups of G of index n, then $\lambda_H \neq \lambda_{H'}$. To this end we observe that the stabilizer of the coset eH of the above action is exactly H ($G_{eH} = \{g \in G \mid gH = H\} = H$). So if $H \neq H'$, then it is the case (due to our labeling of eH as the first coset) that

$$\{g \mid \lambda_H(g) \text{ fixes } 1\} \neq \{g \mid \lambda_{H'}(g) \text{ fixes } 1\},$$

and therefore $\lambda_H \neq \lambda_{H'}$. □

Problem 4.3. Let $N \geq 2$ be an integer. Show that a subgroup of index 2 in S_N is A_N. Here S_N and A_N are the symmetric and alternating groups for N, respectively.

Solution: Let $\sigma \in S_N$. Then $\sigma = \tau_1 \ldots \tau_m$ a product of transpositions (not necessarily unique): If $\sigma(1) = k_1, \ldots, \sigma(N) = k_N$, then $(1\ \ k_1)\sigma$ will send 1 to 1. Similarly, there is a transposition that will ensure $(1\ \ k_1)\sigma$ sends 2 to 2, etc. Therefore

$$(\exists \tau_1, \ldots, \tau_m)\tau_m \ldots \tau_1 \sigma = Id,$$

whence $\sigma = \tau_1 \ldots \tau_m$ since a transposition is its own inverse. Next $\sigma \in S_N$ is even/odd if it can be written as a product of an even/odd number of transpositions. This is well defined: if $\sigma = \tau_1 \ldots \tau_m = \gamma_1 \ldots \gamma_l$ as products of transpositions, consider the polynomial

$$P(\sigma) = \prod_{i<j}(X_{\sigma(i)} - X_{\sigma(j)}).$$

We observe that $P(\tau\sigma) = -P(\sigma)$, where τ is a transposition. From this we conclude that

$$P(\sigma) = (-1)^m P(Id) = (-1)^l P(Id),$$

whence $m \equiv l \pmod 2$. Define $sgn(\sigma) = \pm 1$, depending on whether σ is even or odd. Now let

$$\phi : S_N \longrightarrow \{\pm 1\} : \sigma \mapsto sgn(\sigma).$$

This is a homomorphism since if $\sigma, \tau \in S_N$, $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$: If $sgn(\sigma) = sgn(\tau)$, then $sgn(\sigma\tau) = 1$, otherwise $sgn(\sigma\tau) = -1$. Finally, the kernel of ϕ is exactly A_N, so by the First Isomorphism Theorem

$$S_N/A_N \cong \{\pm 1\},$$

where we view $\{\pm 1\}$ as the group with two elements with 1 equal to the identity. So A_N is a subgroup of index 2 in S_N. $\square$

- First Isomorphism Theorem: Let $f : G \longrightarrow H$ be a group homomorphism. Then

$$Im(f) \cong G/ker(f).$$

- The Symmetric Group on N Objects: The set of permutations of N objects form a group under composition called S_N.
  - S_N is generated by transpositions (each $\tau \in S_N$ can be written as $\gamma_1 \dots \gamma_l$ a product of transpositions where l is unique modulo 2).
  - The set of even permutations form a group of index 2 called A_N.
  - Each $\tau \in S_N$ can be written as a product of disjoint cycles, where a cycle $\sigma = (i_1 \dots i_N)$ means $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_N) = i_1$.
  - The sgn of a cyclic permutation of length p is $p - 1$.