SERGE LANG'S ALGEBRA CHAPTER 1 EXERCISE SOLUTIONS

KELLER VANDEBOGERT

PROBLEM 1

Show that every group of order $\leqslant 5$ is abelian.

The trivial group is abelian. Every group of prime order is cyclic, hence abelian. Finally, for order 4, the only possibilities are $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$, both of which are abelian.

PROBLEM 2

Show that there are two non-isomorphic groups of order 4, namely the cyclic one, and the product of two cyclic groups of order 2.

Note that the only two possibilities for a group of order 4 are $\mathbb{Z}/2 \times \mathbb{Z}/2$ and $\mathbb{Z}/4$. To see this, we observe the order of any elements in our group G if $|G| = 4$. The only possibilities are that there is an order 4 element, in which case we have a cyclic group; the other possibility is that all nonzero elements are order 2 (note that we are using Lagrange's theorem by only looking at the divisors of 4). The latter case yields $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Date: October 22, 2018.

To see that these are nonisomorphic, merely note that any isomorphism must preserve the order of an element. If there were an isomorphism, the image of the order 4 element must remain order 4; this is not possible as there are no order 4 elements in $\mathbb{Z}/2 \times \mathbb{Z}/2$.

PROBLEM 3

Show that the commutator subgroup is a normal subgroups. Show that any homomorphism of G into an abelian group factors through the commutator quotient G/G^c.

It suffices to show $gG^cg^{-1} \subset G^c$ for every $g \in G$. Let $gaba^{-1}b^{-1}g^{-1} \in gG^cg^{-1}$. Letting $[a, b]$ denote the commutator, we see:
$$g[a, b]g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}$$

$$= [g(a), g(b)] \in G^c$$

And normality follows. Suppose now that we have a morphism $\phi : G \to A$ with A abelian. Then,
$$\phi(g)\phi(h) = \phi(h)\phi(g)$$

$$\implies \phi([g, h]) = 1$$

Whence $G^c \subset \operatorname{Ker} \phi$; merely define $\overline{\phi} : G/G^c \to A$ by $\overline{\phi}(gG^c) := \phi(g)$. This is well defined since if $h^{-1}g \in G^c$, then

$$\overline{\phi}(h^{-1}gG^c) = 1 \implies \phi(h) = \phi(g)$$

And well definedness follows.

PROBLEM 4

Let H and K be subgroups of a finite group K with $K \subset N_H$. Show that
$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

By the second isomorphism theorem,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Taking cardinalities,

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Problem 5

Goursat's Lemma. **Let G and G' be groups, let H be a subgroup of $G \times G'$ such that the two projections $p_1 : H \to G$ and $P_2 : H \to G'$ are surjective. Let N be the kernel of p_2 and N' the kernel of p_1. One can identify N as a normal subgroup of G and N' as a normal subgroup of G'. Show that the image of H in $G/N \times G'/N'$ is the graph of an isomorphism**

$$G/N \cong G'/N'$$

In order to show that this is the graph of a homomorphism, we need well definedness. That is, if we have

$$(g_1 N, g_1' N') = (g_2 N, g_2' N') \in \frac{G}{N} \times \frac{G}{N'}$$

with $g_1 N = g_2 N$, then in fact $g_1' N' = g_2 N'$. Firstly, note that by surjectivity we get that $p_1(N)$ and $p_2(N')$ are normal in G and G', respectively. We associate N to the subset $p_1(N) \times \{1\} \trianglelefteq G \times G'$ and N' with $\{1\} \times p_2(N') \trianglelefteq G \times G'$. Now, consider the map

$$\phi : H \to \frac{G}{N} \times \frac{G}{N'}$$
$$(g, g') \mapsto (gN, g'N')$$

This is trivially a homomorphism. Suppose then that $(g_2^{-1}g_1, 1) \in N$; we see

$$(1, g_2'^{-1}g_1') = (g_2, g_2')^{-1}(g_1, g_1')(g_2^{-1}g_1, 1)^{-1}$$

$$\in H$$

Hence $(1, g_2'^{-1}g_1') \in N'$, implying that $g_1'N' = g_2'N'$. Thus, we may define $\psi(g_1 N) = g_1'N'$ if $(g_1, g_1') \in H$. This is surjective since $\psi^{-1}(g_1'N') \ni g_1 N$ whenever $(g_1, g_1') \in H$; by symmetry (that is, just employ the above well-definedness argument), ψ is injective, hence an isomorphism. We conclude that

$$\frac{G}{N} \cong \frac{G'}{N'}$$

PROBLEM 6

Prove that the group of inner automorphisms of a group G is normal in $\mathrm{Aut}(G)$.

Let $\phi \in \mathrm{Aut}(g)$. Let $c_g \in \mathrm{Inn}(G)$ denote an inner automorphism. Let $x \in G$ arbitrary; we have

$$\phi c_g \phi^{-1}(x) = \phi(g\phi^{-1}(x)g^{-1})$$

$$= \phi(g)x\phi(g)$$

$$= c_{\phi(g)}(x) \in \mathrm{Inn}(G)$$

So that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

PROBLEM 7

Let G be a group such that $\mathrm{Aut}(G)$ s cyclic. Prove that G is abelian.

Suppose that $\mathrm{Aut}(G)$ is cyclic. In particular, this implies that $\mathrm{Inn}(G)$ is cyclic. But

$$\frac{G}{Z(G)} \cong \mathrm{Inn}(G)$$

is then cyclic as well, implying that G must be abelian.

PROBLEM 8

Let G be a group and let H and H' be subgroups.

(a) **Show that G is a disjoint union of double cosets.**

(b) **Let $\{c\}$ be a family of representatives for the double cosets. For each $a \in G$ denote by $[a]H'$ the conjugate of $aH'a^{-1}$ of H'. For each c we have a decomposition into ordinary cosets**

$$H = \bigcup_c x_c(H \cap [c]H')$$

where $\{x_c\}$ is a family of elements of H, depending on c. Show that the elements $\{x_c c\}$ form a family of left coset representatives for H' in G.

(a). Define an equivalence relation by $x \sim y \iff HxH' = HyH'$. Choose representatives $C = \{c\}$ for each equivalence class; as the equivalence classes form a partition, we know

$$G = \bigcup_{c \in C} HcH'$$

(b). Define another equivalence relation on elements of H by $x \sim_c y \iff xcH'c^{-1} = ycH'c^{-1}$. Choose representatives $\{x_c\}$ for each $c \in C$. Then,

$$H = \bigcup_{c \in C} x_c\big(H \cap cH'c^{-1}\big)$$

By part (i),

$$G = \bigcup_{c \in C} HcH'$$

$$= \bigcup_{c \in C} \bigcup_{c \in C} x_c \big(H \cap cH'c^{-1} \big) cH'$$

$$= \bigcup_{c \in C} \bigcup_{c \in C} HH' \cap x_c cH'$$

$$= \bigcup_{c \in C} \bigcup_{c \in C} x_c cH'$$

So that $\{x_c c\}_{c \in C}$ is a class of coset representatives.

PROBLEM 9

(a) **Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index.**

(b) **Let G be a group and H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.**

(a). Consider the action

$$G \times \frac{G}{H} \to \frac{G}{H}$$

$$(g, g'H) \mapsto gg'H$$

Consider then the induced permutation representation

$$G \to S_{|G/H|}$$

$$g \mapsto \pi_g$$

Then $\pi_g \equiv \mathrm{Id}$ whenever $gg_iH = g_iH$ for every coset. In particular, $gH = H \implies g \in H$, so that $\mathrm{Ker} \subset H$.

(b). Note that we may find $N_1 \trianglelefteq H_1$, $N_2 \trianglelefteq H_2$ by (a). Then,

$$(N_1 N_2 : N_1) = (N_2 : N_1 \cap N_2)$$

Since N_1 has finite index, we have that $N_1 \cap N_2$ has finite index in N_2. But,

$$(G : N_2) = (G : N_1 \cap N_2)(N_2 : N_1 \cap N_2)$$

$$\implies (G : N_1 \cap N_2) < \infty$$

As $H_1 \cap H_2 \supset N_1 \cap N_2$, we deduce that $(G : H_1 \cap H_2) < \infty$ as well.

PROBLEM 10

Let G be a group and let H be a subgroup of finite index. Prove that there is only a finite number of right cosets of H, and that the number of right cosets is equal to the number of left cosets.

Define a map ϕ between the right and left cosets by $\phi(gH) = Hg^{-1}$.

Let us show well definedness first. If $g_2^{-1}g_1 \in H$; by definition, we have

$$Hg_1^{-1}g_2 = H \implies Hg_1^{-1} = Hg_2^{-1}$$

So this is well defined. Injectivity follows just by reading the above proof backwards.

Let us now prove surjectivity. Given Hg, $\phi(g^{-1}H) = Hg$, so this is surjective. Thus we have that ϕ is a bijection between the left and right cosets, so there are the same number of each. In particular, $(G : H) < \infty$ implies that there must be finitely many right cosets as well.

PROBLEM 11

Let G be a group, and A a normal abelian subgroup. Show that G/A operates on A by conjugation, and in this manner obtain a homomoprhism of G/A into $\operatorname{Aut}(A)$.

We only need show the action of G/A is well defined, when

$$\frac{G}{A} \times A \to A$$

$$(gA, a) \mapsto gag^{-1}$$

Note first that $gag^{-1} \in A$ by normality. Suppose now that $g_1 A = g_2 A$, so that $g_2^{-1} g_1 \in A$. Then, certainly $g_2^{-1} g_1 a g_1 g_2 = a$ because A is abelian, so that $g_1 a g_1^{-1} = g_2 a g_2^{-1}$, yielding well definedness.

Hence we have the association

$$G/A \to \operatorname{Aut}(G)$$

$$gA \mapsto c_g$$

PROBLEM 12

Let G be a group and let H, N be subgroups with N normal. Let γ_x denote conjugation by an element $x \in G$.

(a) **Show that $x \mapsto \gamma_x$ induces a homomoprhism $f : H \to \operatorname{Aut}(N)$.**

(b) **If $H \cap N = 1$ show that the name $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if f is trivial.**

(c) **Conversely let N, H be groups, and let $\psi : H \to \operatorname{Aut}(N)$ be a given homomorphism. Construct a semidirect product as follows. Let G be the set of pairs (x, h) with $x \in N$ and $h \in H$. Define the composition law**

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_1)(x_2), h_1 h_2)$$

Show that this is a group law, and yields a semidirect product of N and H.

(a). Observe first that the association $x \mapsto \gamma_x$ is a homomorphism, since

$$\gamma_{xy} = \gamma_x \circ \gamma_y$$

Now, as N is normal, $\gamma_x(n) = xnx^{-1} \in N$, so that $\gamma_x \in \operatorname{Aut}(N)$ (in other words, normality is the condition that the subgroup is stable under conjugation).

(b). Let ϕ denote our product map. Surjectivity is trivial as $(h, 1) \mapsto h$, $(1, n) \mapsto n$.

For injectivity, suppose $hn = h'n'$. Then $h'^{-1}h = n'n^{-1}$, so $h'^{-1}h \in H \cap N = 1$, so that $h = h'$ and $n = n'$. Suppose now that the map $\mathbf{x} \mapsto \gamma_x$ is trivial for all $x \in H$; we see

$$\phi(xx', yy') = xx'yy'$$
$$= xx'yx'^{-1}x'y$$
$$= xyx'y'$$
$$= \phi(x, y)\phi(x', y')$$

So that ϕ is a homomorphism. Suppose conversely that ϕ is a homomorphism; then

$$\phi\big(x, 1)(1, y)\big) = \phi\big((1, y)(x, 1)\big)$$
$$\implies xy = yx \text{ for all } x \in H, \; y \in N$$

Hence $H \subset C_G(N)$, implying $x \mapsto \gamma_x$ is the trivial morphism.

(c). Let $\psi : H \to \operatorname{Aut}(N)$. Define $(x_1 h_1)(x_2, h_2) := (x_1 \psi(h_1)(x_2), h_1 h_2)$. Then,

$$\big((x_1, h_1)(x_2, h_2)\big)(x_3, h_3) = (x_1 \phi(h_1)(x_2), h_1 h_2)(x_3, h_3)$$
$$= (x_1 \phi(h_1)(x_2)\psi(h_1 h_2)(x_3), h_1 h_2 h_3)$$

And,

$$(x_1, h_1)\big((x_2, h_2)(x_3, h_3)\big) = (x_1, h_1)(x_2\psi(h_2)(x_3), h_2 h_3)$$

$$= (x_1\psi(h_1)(x_2\psi(h_2)(x_3)), h_1 h_2 h_3)$$

$$= (x_1\psi(h_1)(x_2)\psi(h_1 h_2)(x_3), h_1 h_2 h_3)$$

So this is associative. Our inverse is

$$(x, h)^{-1} = (\psi(h^{-1})(x^{-1}), h^{-1})$$

with identity $(1, 1)$. Now, identify N with $(N, 1)$ and H with $(1, H)$; we see

$$(N, 1)(1, H) = (N\psi(H)(1), H) = (N, H)$$

And, $(N, 1) \cap (1, H) = (1, 1)$, so we have an isomorphism

$$N \times H \to NH$$

Problem 13

(a) **Let H and N be normal subgroups of a finite group G. Assume that the order of H and N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \cong HN$.**

(b) **Let $H_1, \ldots, H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that**

$$H_1 \times \cdots \times H_r \cong H_1 \cdots H_r$$

Let $x \in H \cap N$. Then the order of x divides both $|h|$ and $|N|$, so that x has order $1 \implies x = 1$. By the previous problem, this gives that $H \times N \to HN$ is a bijection, and if $xy = yx$, we have an isomorphism. Given $x \in H$, $y \in N$,

$$yxy^{-1} \in H \quad x^{-1}yx \in N$$

But then $x^{-1}yxy^{-1} \in N \cap H = 1$, so

$$x^{-1}yxy^{-1} = 1 \implies xy = yx$$

(b). Proceed by induction, with the base case being part *(a)*. Then,

$$H_1 \times \cdots \times H_n = H_1 \dots H_{n-1} \times H_n$$

$$= H_1 H_2 \dots H_n$$

PROBLEM 14

Let G be a finite groups and let N be a normal subgroup such that N and G/N have relatively prime orders.

(a) **Let H be a subgroup of G having the same order as G/N. Prove that $G = HN$.**

(b) **Let G be an automorphism of G. Prove that $g(N) = N$.**

(a). As H and N have coprime orders, $H \cap N = 1$, so

$$|HN| = |H||N| = \frac{|G|}{|N|} \cdot |N| = |G|$$

Hence $HN = G$.

(b). Let $g \in \mathrm{Aut}(G)$. By definition of automorphism, $|g(N)| = |N|$, so that if $g(N) \neq N$, then $|g(N)|\big||G/N|$. But these orders are coprime, so this is impossible. Hence $g(N) = N$.

PROBLEM 15

Let G be a finite group operating on a finite set S with $|S| \geqslant 2$. Assume that there is only one orbit. Prove that there exists and element $x \in G$ with no fixed point.

Anticipating the result of $19(b)$, note that $|S/G| = 1$ when G acts transitively. Hence,

$$|G| = \sum_{g \in G} |S^g|$$

By definition, $|S^e| > 1$ (where e is the identity), so that $|S^g| = 0$ for at least one $g \in G$. That is, $gs \neq s$ for any $s \in S$.

PROBLEM 16

Let H be a proper subgroup of a finite group G. Show that G is not the union of all of the conjugates of H.

Note that $|G| = k|H|$ for some $k \in \mathbb{N}$ with $k > 1$. Also, $|gHg^{-1}| = |H|$, and we have at most k distinct conjugacy classes of H. Hence, noting that $1 \in gHg^{-1}$ for all $g \in G$, we may choose representatives for each conjugacy class:

$$\left| \bigcup_{i \in I} g_i H h_i^{-1} \right| \leqslant |H|k - k + 1 < |H|k = |G|$$

Hence, G cannot possibly be a union of conjugacy classes.

PROBLEM 17

Let X, Y be finite sets and let X be a subset of $X \times Y$. For $x \in X$, let

$$\phi(x) := \textbf{number of } y \in Y \textbf{ such that } (x, y) \in C$$

Verify that

$$|C| = \sum_{x \in X} \phi(x)$$

This is merely a dual perspective. For each x, let $C_x = \{y \mid (x, y) \in C\}$. Then,

$$C = \bigcup_{x \in X} \{x\} \times C_x$$

And this is a disjoint union since equivalence classes form a partition. Taking cardinalities,

$$|C| = \sum_{x \in X} |C_x|$$

But $|C_x| = \phi(x)$ as defined in the book, hence

$$|C| = \sum_{x \in X} \phi(x)$$

PROBLEM 18

Let S and T be finite sets. Show that $|\mathbf{Map}(S, T) = |T|^{|S|}$.

Let $s \in S$. There are $|T|$ possible ways to map s into T. Over all $s \in S$, we then see that there are $|T|^{|S|}$ maps $S \to T$.

PROBLEM 19

Let G be a finite group acting on a finite set S.

(a) **For each $s \in S$, show that**

$$\sum_{t \in Gs} \frac{1}{|Gt|} = 1$$

(b) **For each $x \in G$ define $f(x) =$ number of elements $s \in S$ such that $xs = s$. Prove that the number f orbits of G in S is equal to**

$$\frac{1}{|G|} \sum_{x \in G} f(x)$$

(a). Note that if $t \in Gs$, then $|Gt| = |Gs|$. Hence,

$$\sum_{t \in Gs} \frac{1}{|Gt|} = \sum_{t \in Gs} \frac{1}{|Gs|}$$
$$= \frac{1}{|Gs|} \sum_{t \in Gs} 1$$
$$= \frac{|Gs|}{|Gs|} = 1$$

(b). We have:

$$|S/G| = \sum_{Gs \in S/G} 1$$
$$= \sum_{Gs \in S/G} \sum_{t \in Gs} \frac{1}{|Gt|}$$
$$= \sum_{s \in S} \frac{1}{|Gs|}$$
$$= \sum_{s \in S} \frac{|G_s|}{|G|}$$
$$= \frac{1}{|G|} \sum_{s \in S} |G_s|$$

Note that

$$\sum_{s \in S} |G_s| = \left| \{(s, g) \mid gs = s\} \right| = \sum_{s \in S} |S^g|$$

Hence, combining this with the above,

$$|S/G| = \sum_{s \in S} |S^g|$$

PROBLEM 20

Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Let $A \trianglelefteq P$. As $|A| = p$, A is cyclic. It suffices to show that $C_G(A) = P$. Consider:

$$\left| \frac{P}{C_G(A)} \right| \; \Big| \; |\mathrm{Aut}(A)| = p - 1$$

But this must imply that $|P| = |C_G(A)|$, since else $p - 1$ would have to have p as a prime factor. This gives that $P = C_G(A)$, so $A \leqslant Z(G)$.

PROBLEM 21

Let G be a finite group and H a subgroup. Let P_H be a p-Sylow subgroup of H. Prove that there exists a p-Sylow subgroup P of G such that $P_H = P \cap H$.

Note that there exists a Sylow p-subgroup containing any p-subgroup of G. If P is a Sylow p-subgroup of H, then P is a p-subgroup of G. By Sylow's theorem, $P \subset P_H$ for some $P_H \in \mathrm{Syl}_p(G)$. By selection, $P \subset P_H \cap H$. Conversely, as $P_H \cap H$ is a subgroup, $p^m \leqslant |P_H \cap H| \big| p^m k$.

As k and p share no factor, it must be that

$$|P_H \cap H| = p^m = |P|$$

As $P \subset P_H \cap H$, we deduce that $P = P_H \cap H$, as desired.

PROBLEM 22

Let H be a normal subgroup of a finite group G and assume that $|H| = p$. Prove that H is contained in every p-Sylow subgroup of G.

As H is a p subgroup, it is contained in some $P \in \mathrm{Syl}_p(G)$. All Sylow p subgroups are conjugate, so given any other $Q \in \mathrm{Syl}_p(G)$, $Q = gPg^{-1}$

for some $g \in G$. But then,

$$H \leqslant P \implies gHg^{-1} \leqslant gPg^{-1} = Q$$

$$\implies H \leqslant Q$$

Where the last step uses normality of H. But then we see that H is contained in all such Sylow p subgroups.

PROBLEM 23

Let P, P' be p-Sylow subgroups of a finite group G.

(a) **If $P' \subset N(P)$, then $P' = P$.**

(b) **If $N(P') = N(P)$, then $P = P'$**

(c) **We have $N(N(P)) = N(P)$.**

(a). By definition, $P \trianglelefteq N(P)$, so that P is the unique Sylow p subgroup of $N(P)$. Hence, if P' is any other Sylow p subgroup, $P' = P$.

(b). If $N(P) = N(P')$, then $P \leqslant N(P')$. But by part (a), we must have that $P = P'$.

(c). Note that $N(P) \subset N(N(P))$ trivially. Suppose $a \in N(N(P))$; we see:

$$P \subset N(P) \implies aPa^{-1} \subset aN(P)a^{-1}$$

$$\implies aPa^{-1} \subset N(P)$$

Since all Sylow p subgroups are conjugate, we know that $aPa^{-1} \in \mathrm{Syl}_p(N(P))$. But P is the unique such subgroup, so that $aPa^{-1} = P \implies a \in N(P)$. Whence

$$N(P) = N(N(P))$$

as desired.

PROBLEM 24

Let p be a prime number. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.

Suppose $|G| = p^2$. Then, $Z(G)$ is nontrivial by the class equation, so we have that $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$, then $G = Z(G)$ and G is trivially abelian.

If $|Z(G)| = p$, then $G/Z(G)$ has order p and is hence cyclic. But this implies G is abelian as well. Hence, since every subgroup must have order dividing p^2, the only two possibilities are

$$G \cong \mathbb{Z}/p^2, \quad G \cong \mathbb{Z}/p \times \mathbb{Z}/p$$

PROBLEM 25

Let G be a group of order p^3, where p is prime, and G is not abelian. Let Z denote the center, and let C be the cyclic group of order p.

(a) **Show that $Z \cong C$ and $G/Z \cong C \times C$.**

(b) **Every subgroup of order p^2 contains Z and is normal.**

(c) **Suppose $x^p = 1$ for all $x \in G$. Show that G contained a normal subgroup $H \cong C \times C$.**

(a). Since G is not abelian, $Z(G) \neq G$. Also, if $|Z(G)| = p^2$, then $G/Z(G)$ is cyclic, in which case G is abelian. By the class equation, $Z(G)$ is not trivial, whence we see that $|Z(G)| = p$, so that $Z(G) \cong C$.

Now, since $|G/Z(G)| = p^2$, the previous problem gives that $G/Z(G) = C \times C$ or $\mathbb{Z}/p^2$. If $G/Z(G) \cong \mathbb{Z}/p^2$, then this is cyclic, and G must be abelian. Thus $G/Z(G) \cong C \times C$.

(b). Firstly, if $|H| = p^2$, then $(G : H) = p$, which is the smallest prime divisor of p^3. Hence, H is normal. Suppose for sake of contradiction that $H \not\supset Z(G)$. Then, $H \cap Z(G) = 1$, in which case $HZ(G) = G$. Note that since $|H| = p^2$, the previous problem gives that it must be abelian. Hence, given $g_1, g_2 \in G$,

$$g_1 = h_1 z_1, \quad g_2 = h_2 z_2, \ h_i \in H, \ z_i \in Z(G)$$

We see:

$$g_1 g_2 = h_1 z_1 h_2 z_2$$

$$= h_1 h_2 z_2 z_1$$

$$= h_2 h_1 z_2 z_1$$

$$= h_2 z_2 h_1 z_1$$

$$= g_2 g_1$$

Implying that G is abelian, which is a contradiction. Therefore, we must have that $H \supset Z(G)$ so all subgroups of order p^2.

(c). We can find some $x \in G$ such that $x \notin Z(G)$. Consider then the subgroup

$$(x) \cdot Z(G) = \{x^n z \mid n \in \mathbb{Z}, \ z \in Z(G)\}$$

Since $Z(G)$ is normal, the above product is a subgroup; since $x \notin Z(G)$, we know that $|(x) \cdot Z(G)| = p^2$. By part (b), $(x) \cdot Z(G) \cong C \times C$ and is normal.

PROBLEM 26

(a) **Let G be a subgroup of order pq, where p and q are primes with $p < q$. Assume that $q \not\equiv 1 \mod p$. Prove that G is cyclic.**

(b) **Show that every group of order 15 is cyclic.**

(a). We first consider the number of Sylow p and q subgroups. Note that for n_p (the number of Sylow p subgroups), $n_p \equiv 1 \mod p$. Since $q \not\equiv 1 \mod p$ and $n_p \in \{1, q\}$, we deduce that $n_p = 1$, so $P \trianglelefteq G$. Similarly, since $p < q$, $n_q = 1$ as well, and $Q \trianglelefteq G$. Both P and Q are cyclic (since they have prime order), and have trivial intersection. Thus, $G = PQ$.

We have the isomorphism $G/C_G(P) \cong \mathrm{Aut}(\mathbb{Z}/p)$, so that

$$\frac{pq}{|C_G(P)|} \Big| p - 1$$

But this is only possible is $|C_G(P)| = pq$, giving that $C_G(P) = G$. Thus, $Q \subset C_G(P)$, and G is abelian. Finally, since P and Q are cyclic, choose respective generators x and y. Then xy has order pq, whence

$$G = (pq)$$

so that G is cyclic.

(b). Note that $15 = 3 \cdot 5$. Setting $p = 3$, $q = 5$, $q \not\equiv 1 \mod 3$, so by part *(a)*, this is cyclic.

Problem 27

Show that every group of order < 60 is solvable.

We proceed by induction on different cases. Assume first that $|G| = 2^m \cdot 3^n$. Then, the base case is of course trivial. For $m \leqslant 3$, $n_3 \in \{1, 4\}$. If $n_3 = 1$, then the Sylow 3 subgroup is normal and cyclic, hence solvable. By induction, G/P is solvable, so that G is also solvable.

If $n_3 = 4$, we have an action of G on $\mathrm{Syl}_3(G)$ by conjugation. Let $\phi : G \to S_4$ be the permutation representation of each element. Then $\mathrm{Im}\, \phi \leqslant S_4$ is solvable, since it is a subgroup of a solvable group. By

the inductive hypothesis, $\operatorname{Ker}\phi$ is solvable, hence, as $\operatorname{Im}\phi \cong G/\operatorname{Ker}\phi$, G must also be solvable.

Now suppose $m \geqslant 4$. If $n = 0$, G is a p group, hence solvable. If $n = 1$, then $m = 4$, so that $|G| = 48$. We have that $n_2 \in \{1, 3\}$. If $n_2 = 1$, we again use normality to proce that G is solvable. If $n_2 = 3$, we have permutation representation $\phi : G \to S_3$ induced by acting on the Sylow subgroups by conjugation. Since S_3 is solvable, so is $\operatorname{Im}\phi$, and by the inductive hypothesis, $\operatorname{Ker}\phi$ is also solvable. Then, $G/\operatorname{Ker}\phi = \operatorname{Im}\phi$, from which we see that G is also solvable.

Now, let p be the largest prime factor of $|G|$. If $p > 7$, then $|G| = pk$ for some $k < p$. As $n_p \cong 1 \mod p$, the only possibility is $n_p = 1$, so the Sylow p subgroup is normal. By induction, it is solvable and so is G/P, so G is also solvable.

When $p = 7$, we see that the only possible value for $|G| < 60$ with $|G| = 7k$, $k > 7$ is $|G| = 56$. Hence, when $k < 8$, the Sylow 7 subgroup is normal, hence solvable. When $k = 8$, $n_7 \in \{1, 8\}$. Assume then that $n_7 = 8$, since if $n_7 = 1$, normality and the inductive hypothesis immediately gives that G is solvable. When $n_7 = 8$, we have $6 \cdot 8 = 48$ elements of order 6, leaving room for only 1 Stlow 2 subgroup. But then this Sylow 2 subgroup is normal, whence G is solvable by induction.

Finally, set $p = 5$. If $k \leqslant 5$ and $|G| = 5k$, then $n_5 = 1$. Whence the Sylow 5-subgroup is normal and by induction, G is solvable. Assume now that $k > 5$. Then, if $k \not\equiv 1 \mod 5$, the above shows G is solvable. Hence, assume $|G| < 60$ and $k \equiv 1 \mod 5$. The only possibility is that $|G| = 30$, and $n_5 \in \{1, 6\}$.

Assume $n_5 = 6$ then, since the other case yields solvability trivially. Then there are $4 \cdot 6 = 24$ elements of order 4, leaving room for only

one Sylow 3 subgroup. Hence, $Q \in \text{Syl}_3(G)$ is normal, and G/Q and Q must be solvable by induction. Thus, G is also solvable.

This exhausts all cases, so we see that every group of order < 60 is solvable.

PROBLEM 28

Let p, q be distinct primes. Prove that a group of order $p^2 q$ is solvable, and that one its Sylow subgroups is normal.

If $p = q$, then G is a p group, hence solvable. Suppose that $p \neq q$, so $p > q$. Then $n_q = 1$, and the unique Sylow q subgroup is normal. But then Q and G/Q are solvable by induction, hence G is.

Now suppose $p < q$. If $n_q = 1$, we are done. Hence $n_q = p^2$. Then, there are $p^2(q-1)$ elements of order q. But then there is only room for a single Sylow p group, so this is normal, and G is solvable.

PROBLEM 29

Let p, q be odd primes. Prove that a group of order $2pq$ is solvable.

If $p = q$, then G is solvable by the previous problem. Assume then that $p < q$. This implies that $n_q \in \{1, 2p\}$. If $n_q = 1$, we are done, so assume $n_q = 2p$. Then, G has $2p(q-1)$ elements of order q.

Now, $n_p \in \{1, q, 2q\}$. If $n_p = 1$, again, we are done, so assume $n_p = q$. Then, there are $q(p-1)$ elements of order p in G. Finally, consider $n_2 \in \{1, p, q, pq\}$. If $n_2 = 1$, we are done, so assume $n_2 = p$.

Now, $p - 1 > 1$, since p is an odd prime; we then see that

$$|G| \geqslant 2p(q-1) + q(p-1) + p$$

$$> 2p(q-1) + q + p$$

$$> 2p(q-1) + p + p$$

$$= 2pq = |G|$$

Which is a contradiction. Hence, G contains at least one normal Sylow subgroup, so that G is solvable.

Problem 30

(a) **Prove that one of the Sylow subgroups of a group of order 40 is normal.**

(b) **Prove that one of the Sylow subgroups of a group of order 12 is normal.**

(a). If $|G| = 40 = 2^3 \cdot 5$, $n_5 \in \{1, 2, 4, 8\}$. The condition $n_5 \equiv 1 \mod 5$ forces $n_5 = 1$ identically, so the Sylow 5 subgroup is normal.

(b). Consider $|G| = 12 = 2^2 \cdot 3$, and the permutation representation of G by the action

$$G \times G/P \to G/P$$

$$(g, aP) \mapsto gaP$$

where $P \in \mathrm{Syl}_2(G)$. If $\phi : G \to S_3$, and $\mathrm{Ker}\,\phi$ is proper and nontrivial, then we are done since the kernel of a map is always normal.

Suppose then that $\mathrm{Ker}\,\phi = G$. Then, since $\mathrm{Ker}\,\phi \leqslant P$, we see that $|G| = |\mathrm{Ker}\,\phi||P| \implies 12|4$, which is impossible. Hence, $\mathrm{Ker}\,\phi$ is a proper nontrivial normal subgroup of G.

PROBLEM 31

Order 1: Trivial

Order 2: $\mathbb{Z}/2$

Order 3: $\mathbb{Z}/3$

Order 4: $\mathbb{Z}/4$ and $\mathbb{Z}/2 \times \mathbb{Z}/2$

Order 5: $\mathbb{Z}/5$

Order 6:

$$\text{Abelian: } \mathbb{Z}/6, \ \mathbb{Z}/2 \times \mathbb{Z}/3$$

$$\text{Nonabelian: } S_3$$

Order 7: $\mathbb{Z}/7$

Order 8:

$$\text{Abelian: } \mathbb{Z}/8, \ \mathbb{Z}/2 \times \mathbb{Z}/4, \ \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$$

$$\text{Nonabelian: } D_8, \ \text{Quaternion group}$$

Order 9: $\mathbb{Z}/3 \times \mathbb{Z}/3$ and $\mathbb{Z}/9$.

Order 10:

$$\text{Abelian: } \mathbb{Z}/10$$

$$\text{Nonabelian: } D_{10}$$

PROBLEM 32

Let S_n be the permutation group on n elements. Determine the p-Sylow subgroups S_3, S_4, S_5 for $p = 2$ and $p = 3$.

(a). S_3: The Sylow 2 subgroups are merely the subgroups generated by the transpositions. The Sylow 3 subgroup is A_3 and is normal.

(b). S_4: The Sylow 3 subgroups are generated by the 3-cycles, and there are 4 of them. The Sylow 2 subgroups are of order 8 and are nonabelian. By the previous problem, they must be isomorphic to D_8,

and since we have 8 elements of order 3 from the Sylow 3 subgroups, there are 3 such copies of D_8.

(c). S_5: The Sylow 3 subgroups are again generated by the 3-cycles, and we have 10 of them. The Sylow 2 subgroups are again isomorphic copies of D_8, so we only need to determine how many copies there are. $n_2 \in \{1, 3, 5, 15\}$, and we see that n_2 must equal 5.

PROBLEM 33

Let σ be a permutation of a finite set I having n elements. Define $e(\sigma)$ to be $(-1)^m$ where

$$m = n - \textbf{number of orbits of } \sigma$$

If $I_1, \ldots, I_r$ are the orbits of σ, then m is also equal to the sum

$$m = \sum_{\nu=1}^{r} \left(|I_\nu| - 1 \right)$$

By definition of orbit, the orbits of σ are disjoint. Hence,

$$|I| = \sum_{v=1}^{r} |I_v|$$

Similarly, the number of orbits is $\phi(\sigma) = \sum_{v=1}^{r} 1$. Hence,

$$m = |I| - \phi(\sigma)$$

$$= \sum_{v=1}^{r} |I_v| - \sum_{v=1}^{r} 1$$

$$= \sum_{v=1}^{r} |I_v| - 1$$

Then it suffices to show that $e(\tau) = -1$. But this is trivial:

$$m = n - (n - 1) = 1$$

So that $e(\tau) = -1$, as asserted. Since any σ can be decomposed as a product of transpositions, we see:

$$e(\sigma) = e(\tau_1 \ldots \tau_k) = (-1)^k = \epsilon(\sigma)$$

So we are done.

PROBLEM 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 $\sigma^n = 1 = \tau^2$ and $\sigma\tau = \tau\sigma^{n-1}$. This group is called the dihedral group.**

(b) **Let n be an off positive integer. Let D_{4n} be the group generated by the matrices**

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

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

(a). Let D_{2n} be the group of rotations and reflections on the vertices of an n-sided regular polygon. σ will be rotation by $2\pi/n$ radians, and τ is a reflection. Then it is geometrically evident that $\tau^2 = 1$, and $\sigma^n = 1$. Also, if we choose base point $1 \in \mathbb{C}$,

$$\sigma\tau(1) = -e^{2\pi i/n}$$
$$= \tau(e^{-2\pi i/n})$$
$$= \tau\sigma^{n-1}(1)$$

Whence $\sigma\tau = \tau\sigma^{n-1}$.

(b). Note

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Also,

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -\xi \\ \xi^{-1} & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -\xi^{1-n} \\ \xi^{n-1} & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \xi^{n-1} & 0 \\ 0 & \xi^{1-n} \end{pmatrix} \\ &= \tau\sigma^{n-1} \end{aligned}$$

PROBLEM 35

Show that there are exactly two nonisomorphic nonabelian groups of order 8**.**

Assume that G is nonabelian of order 8. Then our nonidentity elements have order 2 or 4. If any elements have order 8, G would be cyclic, hence abelian.

If every element have order 2, then

$$(xy)^2 = e \implies xy = yx \text{ for all } x, y \in G$$

so that G would again be abelian. Thus, there exists at least one $g \in G$ with order 4. Now, for $h \in G\backslash(g)$, (g, h) properly contains (g) so that $(g, h) = G$.

Now, $|G/(g)| = 2$, so that $(g) \trianglelefteq G$ and

$$hgh^{-1} \in \{1, g, g^2, g^3\}$$

Since hgh^{-1} has order 4, we deduce that $hgh^{-1} = g$ or $hgh^{-1} = g^{-1}$. In the first case, h and g commute, so G would be abelian. Hence $hgh^{-1} = g^{-1}$. Now, as $|G/(g)| = 2$, $h^2 \in (g)$ and as h has order 2 or 4, h^2 has order 1 or 2, implying

$$h^2 \in \{1, g^2\}$$

In the first case, $G = (h, g)$ with the relations

$$h^2 = 1, \ g^4 = 1, \ hgh^{-1} = g^{-1}$$

But this is precisely D_8. In the second case,

$$h^2 = g^2, \ g^4 = 1, \ hgh^{-1} = g^{-1}$$

and this is precisely the quaternion group, so we are done.

PROBLEM 36

Let $\sigma = (1 \ 2 \ \dots \ n)$ in S_n. Show that the conjugacy class of σ has $(n-1)!$ elements. Show that the centralizer of σ is the cyclic group generated by σ.

Holding 1 fixed, we permute the rest of the elements of the cycle. This gives $(n-1)!$ distinct conjugates. Since σ contains every $\{1, 2, \dots, n\}$, no other cycle is disjoint and hence cannot commute unless it is a power of σ. We deduce that

$$C_{S_n}((\sigma)) = (\sigma)$$

PROBLEM 37

(a) **Let $\sigma = (i_1 \ \dots \ i_m)$ be a cycle. Let $\gamma \mathfrak{n} S_n$. Show that $\gamma \sigma \gamma^{-1}$ is the cycle**

$$(\gamma(i_1) \ \dots \ \gamma(i_m))$$

(b) **Suppose that a permutation σ in S_n can be written as a product of r disjoint cycles, and let $d_1, \ldots, d_r$ be the number of elements in each cycle, in increasing order. Let τ be another permutation which can be written as a product of disjoint cycles whose cardinalities are $d'_1, \ldots, d'_s$ in increasing order. Prove that σ is conjugate to τ in S_n if and only if $r = s$ and $d_i = d'_i$ for all $i = 1, \ldots, r$.**

(a). Since γ is a bijection, any $a \in \{1, \ldots, n\}$ is $\tau(b)$ for some $b \in \{1, \ldots, n\}$. Now assume $b = i_k$ for some k. We see:

$$\tau(i_1 \ \ldots \ i_m)\tau^{-1}(a) = \tau(i_1 \ \ldots \ \tau_m)(i_k)$$

$$= \tau(i_{k+1})$$

$$= (\tau(i_1) \ \ldots \ \tau(i_m))(a)$$

And, if $b \notin \{i_1, \ldots, i_m\}$,

$$\tau(i_1 \ \ldots \ i_m)\tau^{-1}(a) = \tau\tau^{-1}(a) = a$$

In both cases, the result follows.

(b). Let σ_i be our disjoint cycles. Then,

$$\tau\sigma_1 \ldots \sigma_r\tau^{-1} = \tau\sigma_1\tau^{-1}\tau \ldots \tau\sigma_r\tau^{-1}$$

By part (a), the cycle length for each σ_i is preserved, whence the overall cycle type is also preserved.

PROBLEM 38

(a) **Show that S_n is generated by the transpositions (12), $(13), \ldots,$ $(1n)$.**

(b) **Show that S_n is generated by the transpositions (12), (23), $\ldots,$ $(n-1, n)$.**

(c) **Show that S_n is generated by the cycles (12) and $(1\ 2\ \ldots\ n)$.**

(d) **Assume that n is prime. Let $\sigma = (1\ 2\ \ldots\ n)$ and let $\tau = (r\ s)$ be any transposition. Show that σ, τ generate S_n.**

(a). As S_n is generated by transpositions, it suffices to show that an arbitrary transposition is generated by a transposition of the given form. We see

$$(a_1\ a_2) = (1\ a_1)(1\ a_2)(1\ a_1)$$

So that S_n is generated by such transpositions.

(b). By part (a), it suffices to show that transpositions of the form $(1\ k)$ are generated by the given transposition type. We see

$$(1\ k) = (1\ 2)(2\ 3) \ldots (k-1\ k)(k-2\ k-1) \ldots (2\ 3)(1\ 2)$$

(c). By part (b), it suffices to show all transpositions of the type $(k-1\ k)$ are generated by $(1\ 2)$ and $(1\ \ldots\ n)$. Using the result of problem 37, we see

$$(k-1\ k) = (1\ 2 \ldots\ n)^{k-2}(1\ 2)\big((1\ 2\ \ldots\ n)^{k-2}\big)^{-1}$$

Giving the result.

(d). Let $\sigma = (1\ 2\ \ldots\ p)$, $\tau = (r\ s)$. Then, for some power of σ, r and s must be adjacent, and if $r - s = d$, (σ, τ) contains all transpositions of the form $(k - d\ k)$. Then, taking well chosen transpositions, we may reduce the given of the numbers in our transpositions. Using the same process, we get another set of transpositions with length strictly smaller. Continuing this process, we eventually generate all transpositions of the form $(k - 1\ k)$, which, by part (b), generate S_p.

Problem 39

Show that the action of the alternating group A_n on $\{1,\ldots,\,n\}$ is $(n-2)$-transitive.

A_n has a subgroup isomorphic to S_{n-2}, and S_{n-2} is $n-2$ transitive. Also, given $n-1$ distinct elements $\{1,\ldots,n-1\}$, there does not exist $\sigma \in A_n$ sending

$$\{1,\ldots,n-2,n-1\} \mapsto \{1,\ldots,n-1,n-2\}$$

so that A_n is $n-2$ transitive.

Problem 40

Let A_n be the alternating group on $\{1,\ldots,n\}$ and let H_j denote the subgroup of A_n fixing j, so $H_j \cong A_{n-1}$, and $(A_n : H_j) = n$ for $n \geqslant 3$. Let $n \geqslant 3$ and let H be a subgroup of index n in A_n.

(a) **Show that the action of A_n on cosets of H by left translation gives an isomorphism A_n with alternating group of permutations of A_n/H.**

(b) **Show that there exists an automorphism of A_n mapping H_1 on H, and that such an automorphism is induced by an inner automorphism of S_n if and only if $H = H_i$ for some i.**

(a). Enumerate the distinct cosets

$$\{H, \sigma_1 H, \ldots, \sigma_{n-1}H\}$$

And send each $\sigma \in A_n$ to its permutation representation induced by the actions of left coset multiplication. As A_n is simple for $n \geqslant 5$, the kernel must be trivial, so we have an isomorphism (note that the $n < 5$

cases are trivial). It remains to show that π_σ is an even permutation for $\sigma \in A_n$.

Since we have an isomorphism, A_n is isomorphic to its image as a subgroup of S_n; but the only such subgroup is A_n itself, whence every even permutation must have permutation representation that is also even.

(b). We have an isomorphism by part *(a)* sending $A \to \mathrm{Alt}(A_n/H)$. Identify H with the element $1 \in \{1, \ldots, n\}$. Consider the induced isomorphism $A_n \cong \mathrm{Alt}(A_n/H)$, and we may compose the maps

$$A_n \to \mathrm{Alt}(A_n/H) \to A_n$$

to get an automorphism of A_n. Now, the image of $H \leqslant A_n \to \mathrm{Alt}(A_n/H)$ is precisely the set of elements fixing H. Composing this with the second isomorphism, we get an induced isomorphism between the element of A_n fixing 1.

Now, consider S_n acting by conjugation on $\{H_1, \ldots, H_n\}$. If $\sigma \in H_i$, then any $\tau \in S_n$ is such that $\tau\sigma\tau^{-1} \in H_j$, so inner automorphisms merely permute the subgroups $\{H_1, \ldots, H_n\}$. If $H = \tau H_i \tau^{-1}$, the previous sentence tells us $H_i = \tau^{-1}H\tau \implies H \in \{H_1, \ldots, H_n\}$, so we are done.

PROBLEM 41

Let H be a simple group of order 60.

(a) **Show that the action of H by conjugation on the set of its Sylow subgroups induces and embedding $H \hookrightarrow A_6$.**

(b) **Using the preceding exercise, show that $H \cong A_5$.**

(c) **Show that A_6 has an automorphism which is not induced by an inner automorphism of S_6.**

(a). Consider the set of Sylow 5 subgroups. Then, $|\mathrm{Syl}_5(H)|\big|12$ and is congruent to 1 mod 5. Thus it is either 1 or 6. If it is 1, then H is not simple, so we have 6 Sylow subgroups of H. Now consider the conjugation action of $\mathrm{Syl}_5(H)$. This induces a permutation representation in S_6 with trivial kernel by simplicity of S_6. Whence we have an embedding $H \hookrightarrow S_6$, and we want to further argue that the image in contained in A_6.

To see this, consider the elements of order 3 in H, and the subgroup generated by these elements. This is normal in H, hence all of H (and nontrivial by Sylow's theorem). Thus the permutation representation is generated by order 3 elements, hence even, so that $H \hookrightarrow A_6$, as desired.

(b). Counting cardinalities, we see the image of $H \hookrightarrow A_6$ has index 6 in A_6. Also, H is generated by its order 3 elements, implying that $H \cong A_5$.

(c). By the previous problem, it suffices to show that $H \neq H_i$ for any $i \in \{1, \ldots, 6\}$. However, the action of H is induced by conjugation on its Sylow subgroups. If every element of H fixed some Sylow 5 subgroup, then H would have to be simple. Hence, $h \neq H_i$, and we deduce that there exists at least one automorphism of A_6 not induced by any inner automorphism of S_6.

PROBLEM 42

Viewing $\mathbb{Z}$ and $\mathbb{Q}$ 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 $n \geqslant 1$, and that this subgroup is cyclic.

$\mathbb{Q}/\mathbb{Z}$ is a torsion group since for any $p/q \in \mathbb{Q}$, $\frac{p}{q} + \cdots + \frac{p}{q} = 0$ (where we have added this q times). The unique subgroup of order n is $(1/n + \mathbb{Z})$. To see this, suppose that $b + \mathbb{Z}$ has order n. Then, $nb \in \mathbb{Z} \implies b = m/n$ for coprime $m, n \in \mathbb{Z}$. Hence, $(b+\mathbb{Z}) = (1/n+\mathbb{Z})$, and this is certainly cyclic by construction.

PROBLEM 43

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

Theorem 8.1 gives that G is isomorphic to the direct sum of its p-torsion parts, and by Theorem 8.2, these are isomorphic to a product of cyclic p groups. Hence, it suffices to prove the statement when G is a p groups and then induct of the p torsion parts. Now,

$$G = \mathbb{Z}/p^{\alpha_1} \oplus \mathbb{Z}/p^{\alpha_2} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_k}$$

where $1 \leqslant \alpha_1 \leqslant \ldots \leqslant \alpha_k$. Any quotient Q of G is also a p group and hence has a similar decomposition

$$Q = \mathbb{Z}/p^{b_1} \oplus \cdots \oplus \mathbb{Z}/p^{b_j}$$

with $1 \leqslant b_1 \leqslant \ldots \leqslant b_j$, and $j \leqslant k$. Consider now $\mathbb{Z}/p^{b_j}$ and note that the order of ant element in G is at most p^{a_k}, and likewise for the quotient. This gives that $b_j \leqslant a_k$, and inductively, $b_{j-i} \leqslant a_{k-i}$ for each $i = 1, \ldots, j-1$. Now, at each step, we may find a cyclic subgroup of

order $p^{b_j - i}$ of G (since we are working with cyclic groups), and hence, taking the direct sum of all of the above,

$$\mathbb{Z}/p^{b_1} \oplus \cdots \oplus \mathbb{Z}/p^{b_j}$$

is our constructed subgroup, and this is isomorphic to the original quotient as contended.

Problem 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 sese that if two of these three indices are finite, so is the third, and the stated equality holds.

We have the inclusion $A_f / B_f \hookrightarrow A/B$, with $a + B_f \mapsto a + B$, and similarly a surjection

$$\phi : A/B \to A^f / B^f$$

sending $a + B \mapsto f(a) + B^f$. If $a + B_f \in A_f / B_f$, then $f(a) + B_f = B_f$; that is, $A_f / B_f \subset \operatorname{Ker} \phi$. By the first isomorphism theorem, we see that

$$\frac{A/B}{\operatorname{Ker} \phi} = \frac{A^f}{B^f}$$

So that

$$|\operatorname{Ker} \phi| = \frac{|A|/|A^f|}{|B|/|B^f|} = \left| \frac{A_f}{B_f} \right|$$

Whence $\operatorname{Ker} \phi = A_f / B_f$, and,

$$\frac{A^f}{B^f} = \frac{A/B}{A_f / B_f}$$

Taking orders of the above,

$$(A : B) = (A^f : B^f)(A : B)$$

as desired.

PROBLEM 45

Let G be a finite cyclic group of order n, generated by σ. Assume that G operates on an abelian group A, and let $f, g : A \to A$ be the endomorphisms of A given by

$$f(x) = \sigma(x) - x, \quad g(x) = x + \sigma(x) + \cdots + \sigma^{n-1}(x)$$

Define the Herbrand Quotient by the expression $q(A) = (A_f : A^g)/(A_g : A^f)$, provided both indices are finite.

(a) **Define in a natural way an operation of G on A/B.**

(b) **Prove that**

$$q(A) = q(B)q(A/B)$$

(c) **If A is finite, show that $q(A) = 1$.**

We have the natural action
$$G \times A/B \to A/B$$
$$(\sigma, a + B) \mapsto \sigma(a) + B$$
Let us show well definedness. If $a + B = a' + B$, then $a - a' \in B \implies \sigma(a - a') \in \sigma(B) \subset B$. Hence,

$$\sigma(a) - \sigma(a') \in B \implies \sigma(a) + B = \sigma(a') + B$$

So this is well defined.

(b). Since $f \circ g = g \circ f = 0$, we may define a complex $\mathcal{C}(A)$ with $A_n = A$ for all $n \in \mathbb{N}$ and differentials

$$d = \begin{cases} f, & n \text{ even} \\ g, & n \text{ odd} \end{cases}$$

By the action defined in part (a), $\mathcal{C}(A/B)$ is also a complex, and we have an exact sequence

$$0 \longrightarrow \mathcal{C}(B) \longrightarrow \mathcal{C}(A) \longrightarrow \mathcal{C}(A/B) \longrightarrow 0$$

of chain complexes. We now want to consider the induced long exact homology sequence, where we note that by periodicity of our differentials,

$$H_p(-) = \begin{cases} H_0(-), & p \text{ even} \\ H_1(-), & p \text{ odd} \end{cases}$$

So we have

$$\cdots \longrightarrow H_1(B) \xrightarrow{i_*} H_1(A) \xrightarrow{\pi_*} H_1(A/B)$$

$$\xrightarrow{\delta} H_0(B) \xrightarrow{i_*} H_0(A) \xrightarrow{\pi_*} H_0(A/B) \longrightarrow 0$$

Then, note that the Herbrand quotient is precisely

$$\frac{|H_0(A)|}{|H_1(A)|}$$

As i_* is injective by definition, we may extract the short exact sequences

$$0 \longrightarrow H_0(B) \xrightarrow{i_*} H_0(A) \xrightarrow{\pi_*} \operatorname{Coker} i_* \longrightarrow 0$$

$$0 \longrightarrow H_1(B) \xrightarrow{i_*} H_1(A) \xrightarrow{\pi_*} \operatorname{Coker} i_* \longrightarrow 0$$

By exactness, $\operatorname{Im} i_* = \operatorname{Ker} \pi_*$, so that

$$|H_0(A)| = |H_0(B)||\operatorname{Im} \pi_{0*}|$$

$$|H_1(A)| = |H_1(B)||\operatorname{Im} \pi_{1*}|$$

Similarly,

$$|H_0(B)| = |\operatorname{Im} \delta_0||\operatorname{Im} i_{0*}|$$

$$|H_1(B)| = |\operatorname{Im} \delta_1||\operatorname{Im} i_{1*}|$$

And

$$H_0(A/B)| = |\operatorname{Im} \pi_{0*}||\operatorname{Im} \delta_1|$$

$$H_1(A/B)| = |\operatorname{Im}\pi_{1*}||\operatorname{Im}\delta_0|$$

Noting that $|\operatorname{Im}\delta_0| = |H_0(B)|$, $|\operatorname{Im}\delta_1| = |H_1(B)|$,

$$
\begin{aligned}
q(B)q(A/B) &= \frac{|\operatorname{Im}\delta_0||\operatorname{Im}i_{0*}|\cdot|\operatorname{Im}\pi_{0*}||\operatorname{Im}\delta_1|}{|\operatorname{Im}\delta_1||\operatorname{Im}i_{1*}|\cdot|\operatorname{Im}\pi_{1*}||\operatorname{Im}\delta_0|} \\
&= \frac{|\operatorname{Im}i_{0*}||\operatorname{Im}\pi_{0*}|}{|\operatorname{Im}i_{1*}||\operatorname{Im}\pi_{1*}|} \\
&= \frac{|H_0(A)|}{|H_1(A)|} \\
&= q(A)
\end{aligned}
$$

As desired.

(c). In the finite case,

$$
\begin{aligned}
q(A) &= \frac{|A_f|/|A^g|}{|A_g|/|A^f|} \\
&= \frac{|A_f||A^f|}{|A_g||A^g|} \\
&= \frac{|A|}{|A|} = 1
\end{aligned}
$$

PROBLEM 46

Let G operate on a set S. Let $S = \bigcup S_i$ be a partition of S into disjoint subset. We say that the partition is stable under G if G maps each S_i onto S_j for some j, and hence G induces a permutation on the sets of the partition among theselves. THere are two partition of S which are obviously stable: the partition consisting of S itself, and the partition consisting of the subsets with one element. Prove that the following two conditions are equivalent:

(1) The only partitions of S which are stable are the two partitions mentioned above.

(2) **If H is the isotropy group of an element of S, then H is a maximal subgroup of G.**

We prove $1 \implies 2$ first. Suppose that G acts transitively, and let H stabilize $s \in S$. We have the surjective map

$$G \to S$$

$$g \mapsto g \cdot s$$

with kernel H, so that $G/H \to S$ is an isomorphism. If there exists $H' \neq G$ containing H, then $G/H' \leqslant G/H$. Restricting the above, we have an induced partition

$$\{gH' \cdot s\}, \quad g \in G$$

Since $|G/H'| < |G/H|$, this is a nontrivial partitition that is stable, contradicting the assumption. Hence H is maximal.

For $2 \implies 1$, argue by contraposition. Suppose we have a nontrivial stable partition, and choose $s \in S$ such that $s \in S_i$ for some S_i in out partition, and $S_i \neq \{s\}$. Let H' be the stabilizer of S_i. Then $H \leqslant H'$ because our partition is stable by assumption. But then H is not maximal, since H' properly contains it, and we are done.

Problem 47

Let a finite group G operate transitively and faithfully on a set S with at least 2 elements and let H be the isotropy group of some element $s \in S$. Prove the following:

(a) **G is doubly transitive if and only if H acts transitively on the complement of s in S.**

(b) **G is doubly transitive if and only if $G = HTH$, where T is a subgroup of G of order 2 not contained in H.**

(c) **If G is doubly transitive and $(G : H) = n$, then**

$$|G| = d(n-1)n$$

where d is the order of the subgroup fixing two elements. Furthermore, H is a maximal subgroup of G, that is, G is primitive.

(a). Let H be the stabilizer of $s \in S$, and suppose first that G is doubly transitive. We have the induced bijection $G/H \to S$, so we may think of G as acting by left mulitplication on G/H. Since G is doubly transitive, the action

$$H : \{H\} \times G/H \to \{H\} \times G/H$$

is surjective. However, we may then ignore the first coordinate to see that H acts transitively on $G/H \backslash \{H\} = S \backslash \{s\}$.

Conversely, let H act transitively on $S \backslash \{s\}$, that is, for any $a, b \notin H$, there exists $h \in H$ such that

$$haH = bH$$

Now let (aH, bH), $(a'H, b'H)$ be two arbitrary pairs. By transitivity of G, we may assume that $aH = a'H = H$. Then, by H transitivity, we may find $h \in H$ such that $hbH = b'H$, whence G is doubly transitive.

(b). Suppose first that G is doubly transitive. Choose $a \neq b \in S$. We first want to show there exists an element of order 2 not contained in H.

Find $g \in G$ such that $(a, b) \mapsto (b, a)$, so that $g^2(a, b) = (a, b)$. Then, g is an involution, and in particular G must have even order. Then the set of elements of order 2 is nonempty. Suppose now that $K \subset H$. If

$x \in K$, then $gxg^{-1} \in K$, so K is stable under conjugation. Hence, if $K \subset H$, then

$$K \subset gHg^{-1}$$

for all $g \in G$, in which case

$$K \subset \bigcap_{g \in G} gHg^{-1} = \varnothing$$

Where the above is empty because G acts faithfully. Thus there exists $t \in K$ with $t \notin H$. Choose $g \notin H$ and by part (a) we can find $h \in H$ such that

$$htH = gH$$

Taking the preimage under this projection, we see that $G \backslash H \subset HTH$, where $T = (t)$. If $g \in H$, then $g = gt^2 \cdot 1 \in HTH$, so we are done.

Conversely, if $G = HTH$ with $T = (t)$, $t^2 = 1$, then H acts transitively on the set of cosets htH, $h \in H$. By part (a), this implies that G is doubly transitive, as desired.

(c). First observe that since $(G : H) = n$, $|S| = n$ since H is the stabilizer. Note that we can count the cardinality of $S \times S$ in two ways. Counting cardinalities, $|S \times S| = n^2$, but $S \times S$ also consists of the diagonal elements along with the nondiagonal elements.

G acts doubly transivitively, so that the number of nondiagonal elements is $|G|/|\operatorname{Ker}|$. But the cardinality of the kernel is precisely d. Hence

$$n^2 = n + \frac{|G|}{d} \implies |G| = d(n-1)n$$

In remains to show that H is maximal. Argue by contraposition. If H is not maximal, choose

$$H \subset H' \subset G$$

and $h' \in H'\backslash H$, $g \in H\backslash H'$. If H stabilizes $s \in S$, then gs and $h's$ are distinct elements $\neq s$. In view of (a), it suffices to show that $gs \neq hh's$ for any $h \in H$.

However, if $gs = hh's$, we see

$$g^{-1}hh' \in H \subset H'$$

$$\implies g^{-1}hh'H' = H'$$

$$\implies gH' = H'$$

$$\implies g \in H'$$

Which is a contradiction. Hence, H does not act transitively on $S\backslash\{s\}$, so that G is not doubly transitive.

PROBLEM 48

Let G be a group acting transitively on a set S with at least 2 elements. For each $x \in G$ let $f(x) =$ number of elements of S fixed by x. Prove:

(a) $\sum_{x \in G} f(x) = |G|$

(b) G is doubly transitive if and only if

$$\sum_{x \in G} f(x)^2 = 2|G|$$

(a). This is merely Burnside's Lemma. Since G acts transitively, there is only one orbit, so that

$$1 = \frac{1}{|G|} \sum_{x \in G} f(x)$$

$$\implies |G| = \sum_{x \in G} f(x)$$

(b). Since G is doubly transitive, there are two orbits of the action of G and its complement. Consider now the order of the fixed points. If

g fixes (a, b), then g fixes a and b. In the problem's notation, this says that there are $f(g) \cdot f(g)$ fixed points of g, so, by Burnside's Lemma,

$$2|G| = \sum_{x \in G} f(x)^2$$

PROBLEM 49

A group as an automorphism group. Let G be a group and let $Set(G)$ be the categoryof G-sets (ie sets with a G-action). Let $F : Set(G) \to Set$ be the forgetful functor. Show that $\mathrm{Aut}(F)$ is naturally isomorphic to G.

Let us define

$$\phi : \mathrm{Aut}(F) \to G$$

$$a \mapsto a_G(1)$$

$$\psi : G \to \mathrm{Aut}(F)$$

where $\psi(g)_x(x) := g \cdot x$. Then,

$$\phi(a \circ b) = (a \circ b)_G(1)$$

$$= a_G(b_G(1))$$

$$= a_G(1)b_G(1)$$

$$= \phi(a)\phi(b)$$

$$\psi(g \cdot g')_x(x) = (g \cdot g') \cdot x$$

$$= g(g'x)$$

$$= \psi(g)_x \psi(g')_x(x)$$

So, ϕ and ψ are indeed homomorphisms of groups. It remains to show that ϕ and ψ are inverses for each other.

We see:

$$\phi(\psi(g)) = \psi(g)_G(1)$$

$$= g \cdot 1 = g$$

And, for $a \in \mathrm{Aut}(F)$,

$$\psi(\phi(a))_x(x) = \psi(a_G(1))_x(x)$$
$$= a_G(1) \cdot x$$
$$= a_x(x)$$

So we have an isomorphism $\mathrm{Aut}(F) \cong G$.

PROBLEM 50

(a) **Show that fiber products exist in the category of abelian groups.**

(b) **Show that the pullback of a surjective morphism of groups is surjective.**

(a). We only need to show that $X \times_Z Y$ satisfies the universal property guaranteed by the pullback.

Let p_1, p_2 be the natural projections. Assume there exists Q satisfying $f q_1 = g q_2$. Then we may define $u : Q \to X \times_Z Y$ by

$$u(q) = (q_1(q), q_2(q))$$

This is trivially well defined and unique, so we see that $X \times_Z Y$ satisfies the universal property of the pullback.

(b). Let $f : X \to Z$ be surjective. Then, suppose we have $g : Y \to Z$ and the induced projection $p_2 : X \times_Z Y \to Y$. We wish to show that p_2 is a surjection. Let $yinY$. THen, there exists $x \in X$ such that $f(x) = g(y)$, and the pair (x, y) is an element of $X \times_Z Y$. We then see that $p_2(x, y) = y$, so p_2 is surjective.

Problem 51

(a) **Show that fiber products exist in the category of sets.**

(b) **In any category $\mathcal{C}$, consider the category $\mathcal{C}_Z$ of objects over Z. Let $h : T \to Z$ be a fixed object in this category. Let F denote the functor**

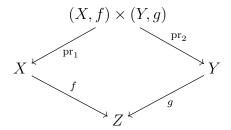$$F(X) = \mathrm{Hom}_Z(T, X)$$

where X is an object over Z. Show that F transforms fiber products into products in the category of sets.

(a). This proof is identical to the proof given in part (a) of the above, noting that we do not have any kind of group structure. That is,

$$X \times_Z Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}$$

(b). Consider a product in the category of objects over Z, that is, $\mathcal{C}_Z$. We have (X, f), (Y, G) as objects, and,

commutes. That is, a product in the slice category over Z is precisely the fiber product over Z. But $\mathrm{Hom}_Z(T, -)$ preseves products, so we deduce that $\mathrm{Hom}_Z(T, -)$ applied to a pullback yields a product in the category of sets.

Problem 52

(a) **Show that pushouts exist in the category of abelian groups.**

(b) **Show that the pushout of an injective morphism of groups is injective.**

(a). Let

$$f : Z \to X$$

$$g : Z \to Y$$

Define

$$X \oplus_Z Y := X \oplus Y / \{(f(z), -g(z)) \mid z \in Z\}$$

Now, in order to construct this, we ask that

$$
\begin{array}{ccc}
Z & \xrightarrow{\;\;g\;\;} & Y \\
{\scriptstyle f}\downarrow & & \downarrow{\scriptstyle i_2} \\
X & \xrightarrow[\;\;i_1\;\;]{} & X \oplus_Z Y
\end{array}
$$

commutes. This is trivially well defined since the q_i are, and we see that the universal property is satisfied.

(b). Suppose that $f : Z \to X$ is injective. We want to show the inclusion

$$i_2 : Y \to X \oplus_Z Y$$

is also injective. Let $y \in \operatorname{Ker} i_2$, so that $(0, y) \in W$. Then,

$$(0, y) = (f(z), -g(z))$$

for some $z \in Z$. But then $f(z) = 0$, and by injectivity, $(z = 0$, so that $y = g(0) = 0$, proving injecivity of i_2.

PROBLEM 53

Let H, G, G' **be groups, and let**

$$f : H \to G, \quad g : H \to G'$$

be two homomorphisms. Define the notion of a coproduct of these two homomorphisms.

We merely take our coproduct as the set $G * G$ (the free product) with the standard inclusions, modulo the set of pairs $(f(h), g(h)^{-1})$, $h \in H$. By the universal property of the free product, we see that the above satisfies the coproduct universal property for our constructed set.

PROBLEM 54

Let G be a group and let $\{G_i\}_{i \in I}$ be a family of subgroups generating G. Suppose G operates on a set S. For each $i \in I$, suppose given a subset S_i of S, and let s be a point of $S \backslash \bigcup_i S_i$. Assume that for each $g \in G_i \backslash \{e\}$, we have

$$g S_j \subset S_i \text{ for all } j \neq i, \quad \text{and } g(s) \in S_i \text{ for all } i$$

Prove that G is the coproduct of the family $\{G_i\}_{i \in I}$.

Following the hint, we suppose that $s \in S \backslash \bigcup_{i \in I} S_i$, and

$$g_1 \cdot \cdots \cdot g_m = \text{id}$$

where $g_i \in G_{ki}$. Then, in this is the case,

$$g_1 \ldots g_m(s) = s$$

and the above implies $s \in S_{ki}$, which is impossible. Hence, no product of elements in the G_i stabilizes s, so no product could possibly we the identity. Following Proposition 12.4, we deduce that G must be the coproduct of the G_i.

PROBLEM 55

Let $M \in GL_2(\mathbb{C})$ act on $\mathbb{C}$ by linear fractional transformations. Let λ and λ' be the eigenvales of M viewed as a linear map on $\mathbb{C}^2$. Let W, W' denote the corresponding eigenvectors. By a fixed point of M we mean a complex number z such that $M(z) = z$. Assume that M has two distinct fixed points $\neq \infty$.

(a) **Show that there cannot be more than two fixed points and that these fixed points are $w = w_1/w_2$ and $w' = w_1'/w_2'$.**

(b) **Assume that $|\lambda| < |\lambda'|$. Given $z \neq w$, show that**

$$\lim_{k \to \infty} M^k(z) = w'$$

(a). A fixed point is such that

$$\frac{az+b}{cz+d} = z \implies cz^2 + (d-a)z - b = 0$$

This is a quadratic in z, hence has at most 2 distinct roots. Now, normalize our eigenvectors to be of the form $\begin{pmatrix} w \\ 1 \end{pmatrix}$, $\begin{pmatrix} w' \\ 1 \end{pmatrix}$. By definition,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} w \\ 1 \end{pmatrix}$$

Implying that $aw + b = \lambda w$, $cw + d = \lambda$. Hence,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} w = w$$

And similarly for w'. Thus we conclude that λ and λ' are the unique fixed points.

(b). We may diagonalize our matrix as

$$M = \begin{pmatrix} w & w' \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix} \begin{pmatrix} w & w' \end{pmatrix}^{-1}$$

Then,

$$\lim_{k \to \infty} M^k(z) = \lim_{z \to \infty} \begin{pmatrix} w & w' \end{pmatrix} \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda'^k \end{pmatrix} \begin{pmatrix} w & w' \end{pmatrix}^{-1}$$

$$= \lim_{k \to \infty} \begin{pmatrix} w & w' \end{pmatrix} \left(\frac{\lambda}{\lambda'} \right)^k \left(\frac{z - w}{-z - w'} \right)$$

$$= \begin{pmatrix} w & w' \\ 1 & 1 \end{pmatrix} (0) = w'$$

So that $\lim_{k \to \infty} M^k(z) = w'$, as desired.

Problem 56

Let $M_1, \ldots, M_r \in GL_2(\mathbb{C})$. be a finite number of matrices. Let λ_i, λ_i' be the eigenvalues of M_i. Assume that each M_i has two distinct complex fixed points and $|\lambda_i| < |\lambda_i'|$. Also assume that the fixed points for $M_1, \ldots, M_r$ are all distinct from each other. Prove that there exists a positive integer k such that $M_1^k, \ldots, M_r^k$ are the free generators of a free subgroup of $GL_2(\mathbb{C})$.

Choose our fixed points w_i, w_i' for each $M_i \in \mathrm{GL}_2(\mathbb{C})$. By the previous problem, for any $z \in \mathbb{C}$ we may find $n_i \in \mathbb{N}$ such that $M_i^{n_i}(z) \in U_i \cap U_i'$. In particular, choose n_i large enough that

$$M_i^{n_i}(s) \in U_i \cap U_i'$$

and, for every other j,

$$M_i^{n_i}(U_J \cap U_J') \subset U_i \cap U_i'$$

Doing this for every $i = 1, \ldots, r$, choose $k := \max_i\{n_i\}$. By construction, the sets $G_i := (M_i^k)$ satisfy

$$gU_j \cap U_j' \subset U_i \cap U_i', \quad g(s) \in U_i \cap U_i'$$

for every $g \in G_i \backslash \{1\}$, over all $i = 1, \ldots, r$. By problem 54, these generate a free subgroup of $\mathrm{GL}_2(\mathbb{C})$.

PROBLEM 57

Let G be a group acting on a set X. Let Y be a subset of X. Let G_Y be the subset of G consisting of those elements g such that $gY \cap Y$ is not empty. Let $\overline{G_Y}$ be the subgroup generated by G_Y. Show that $\overline{G_Y}Y$ and $(G \backslash \overline{G_Y})Y$ are disjoint.

Argue by contraposition. Choose $g_1 \in \overline{G_Y}$ and $g_2 \in G \backslash \overline{G_Y}$ such that $g1y_1 = g_2y_2$ for some $y_i \in Y$. Then, we see that $g_2^{-1}g_1y_1 = y_2$, so that $g_2^{-1}g_1 \in G_Y$, and in particular, as $g_1 \in \overline{G_Y}$, we deduce that $g_2 \in \overline{G_Y}$ as well.