1. Let Γ_n be the group with presentation

$$\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| > 1. \rangle$$

This group is also known as the braid group on n strands. Let Δ denote the element

$$\Delta = \sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_2\sigma_1).$$

It is a fact that the center of Γ_n is infinte cyclic with generator Δ^2.

(a) Compute the abelianization of Γ_n.

Abelianization

There is always a group homomorphism $h: G \to G'$ to an abelian group, and this homomorphism is called Abelianization. The homomorphism is abstractly described by its kernel, the commutator subgroup $[G,G]$, which is the unique smallest normal subgroup of G such that the quotient group $G' = G/[G,G]$ is abelian.

Roughly speaking, in any expression, every product becomes commutative after abelianization.

Some previously unequal expressions may become equal, or even represent the identity element

What the abelianization amounts to is adding a relation that the generators commute

If $\sigma_i\sigma_j = \sigma_j\sigma_i \ \forall\, i,j$, then the braid relation gives

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$
$$\Rightarrow \quad \sigma_i^2\sigma_{i+1} = \sigma_i\sigma_{i+1}^2$$
$$\Rightarrow \quad \sigma_i = \sigma_{i+1}$$

We don't need to take any other relations into account since the generators already commute for $|i-j|>1$.

So we get $\sigma_i = \sigma_j \ \forall\, i,j$, so the group is generated by one element with essentially no relations. So $\Gamma_n^{ab} = \mathbb{Z}$.

Note that this answer is independent of n

(b) Using this fact, prove that Γ_n is not isomorphic to Γ_m if $n \neq m$.

Assume we have an isomorphism $\varphi: \Gamma_n \to \Gamma_m$.

Then $\varphi(\Delta_n^2) = \Delta_m^{\pm 2}$

An isomorphism preserves the center (generator of $Z(\Gamma_n)$ maps to generator of $Z(\Gamma_m)$)

The generators of the center of Γ_m are Δ_m^2 and $(\Delta_m^2)^{-1}$

Now φ induces an isomorphism

$$\tilde{\varphi}: \Gamma_n^{ab} \to \Gamma_m^{ab}$$

So $\tilde{\varphi}: \mathbb{Z} \to \mathbb{Z}$, and therefore $\tilde{\varphi} = \pm \mathrm{id}$

$\Gamma_n^{ab} = \Gamma_m^{ab} = \mathbb{Z}$, and the only isomorphisms $\mathbb{Z} \to \mathbb{Z}$ are $\pm \mathrm{id}$

What happens to Δ_n^2 when it is passed through the abelianization?

$$\Delta_n^2 = \left[\sigma_1(\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_2\sigma_1)\right]^2 = 2\sum_{i=1}^{n-1} i = 2\binom{n}{2} = n(n-1) \quad \text{in } \mathbb{Z}$$

every generator maps to 1 in $\mathbb{Z} = \Gamma_n^{ab}$

Thus we get $n(n-1) = \pm m(m-1)$.

This implies $n = m$ ← the function $f(x) = x(x-1)$ is injective on $\mathbb{N}$

2. Let G be a finite group, and write $|G| = p^a m$, where p is prime and m is relatively prime to p. Prove that for every $0 \leq b \leq a$, G has a subgroup of order p^b. Further prove that if P_b is a subgroup of order p^b, then there is some subgroup P_{b+1} of order p^{b+1} such that $P_b \triangleleft P_{b+1}$.

Solution

We proceed by induction on b.
The base case $b=1$ follows directly from Cauchy's theorem.
Now suppose we have constructed P_b of order b for some $1 \leq b \leq a-1$.

Cauchy's Theorem
If G is a finite group and p is a prime dividing the order of G, then G contains an element of order p.

Normalizer
For a subset $A \subseteq G$, the normalizer of A $N_G(A) = \{g \in G \mid gag^{-1} \in A \text{ for all } a \in A\}$ is the set of elements of G which normalize A

- A subgroup $N \leq G$ is normal in G iff $N_G(N) = G$
- If $A \leq B$ are subgroups of G, then $A \triangleleft B$ iff $B \leq N_G(A)$

Let $N_b = N_G(P_b)$

Claim: $[N_b : P_b] \equiv 0 \mod p$ ← This implies $P_b \neq N_b$, and that $|N_b/P_b|$ has p as a divisor

Proof
Let $X = G/P_b$ ← the set of cosets of P_b ← This may not be a group since P_b may not be normal in G

Let P_b act on X by left multiplication ← This action is not trivial because P_b is not normal

In other words, how many elements are fixed by the entire action of P_b?

How many orbits of size 1?
xP_b is fixed by P_b iff
$gxP_b = xP_b \quad \forall g \in G$
$\iff x^{-1}gx \in P_b \quad \forall g \in G$
$\iff x \in N_b$
So there are $[N_b : P_b]$ orbits of size 1.

The Class Equation
If G is a group acting on a set X, then X is partitioned by the G-orbits.
So, if X is finite, we have the following equivalent equations:

$$|X| = \sum_{x \in X/G} |\text{Orb}(x)|$$

$$|X| = \begin{pmatrix} \#\text{ of orbits} \\ \text{of size } 1 \end{pmatrix} + \sum_{x \in \Omega} |\text{Orb}(x)|$$

where Ω is the set of orbits of size greater than 1.

So we get $|X| = [N_b : P_b] + \sum_{x \in \Omega} |\text{Orb}(x)|$
- $|X| = [G : P_b]$ divisible by p, since
- $\text{Stab}(x) \neq G$ divisible by p, since

Thus we get that $[N_b : P_b]$ is divisible by p.

Orbit-Stabilizer Theorem
If G is a group acting on a finite set X, then for $x \in X$,

$$|\text{Orb}(x)| = [G : \text{Stab}(x)] = \frac{|G|}{|\text{Stab}(x)|}$$

Now, since $|N_b/P_b|$ has p as a divisor, by Cauchy's theorem we know that N_b/P_b has a subgroup $\overline{P}_{b+1}$ of order p.

$\overline{P}_{b+1}$ lifts to a subgroup P_{b+1} of N_b, and $[N_b : P_{b+1}] = [N_b/P_b : \overline{P}_{b+1}] \Rightarrow |P_{b+1}| = p^{b+1}$.

Since $P_{b+1} \subseteq N_b$, we have $P_b \triangleleft P_{b+1}$ as desired.

3. (August 2014 Problem 2) Let G be a finite group, and let A be a subgroup of $Aut(G)$.

(a) Suppose G is the cyclic group $\mathbb{Z}/6\mathbb{Z}$ and A is the full automorphism group. What are the orbits of the action of A on G?

The only automorphisms of $\mathbb{Z}/6\mathbb{Z}$ are $\pm 1_d$
So we have the orbits $\{0\}, \{1,5\}, \{3\}, \{2,4\}$

generators map to generators, and the only generators are ± 1

(b) Let G be a non-trivial finite group. Show that two elements in the orbit of A on G must have the same order.

If a,b are in the same orbit, then there is $\varphi \in A$ with $\varphi(a)=b$. Let $|a|=m$, $|b|=n$.
We have $1=\varphi(1)=\varphi(a^m)=b^m \Rightarrow n \leq m$.
Replacing φ with φ^{-1} we get $m \leq n$.

(c) Show that for any non-trivial finite group G there are always at least two orbits of A on G. Prove that there are exactly two orbits for some A if and only if G is an elementary abelian p-group for some prime p.

Since 1 is always in its own orbit, any nontrivial group has at least two orbits

A p-group G is elementary if $a^p=1$ for all $a \in G$.

($\Rightarrow$) Assume there is $A \leq Aut(G)$ such that $A \curvearrowright G$ has 2 orbits. Then by part (b), all non-trivial elements have the same order.

Cauchy's theorem implies there is only one prime divisor of $|G|$, and all elements have order p.

We want to show that G is abelian.
We show that $G = Z(G)$.
Assume $G \neq Z(G)$. Then there is $a \in G - Z(G)$. Now let $b \in Z(G) - \{1\}$.
By assumption, a and b are in the same orbit, and so there is an automorphism $\varphi \in A$ such that $\varphi(a)=b$. This contradicts the fact that automorphisms preserve the center.
Thus G is abelian.

Theorem: Every p-group has nontrivial center.

($\Leftarrow$) Conversely, let G be an elementary abelian p-group.
Take $A = Aut(G)$. ← The bigger the set of automorphisms, the fewer orbits.

We want to show that any two nontrivial elements are connected by an automorphism.

Since G is finite and abelian, with every element of order p, we must have $G = (\mathbb{Z}/p\mathbb{Z})^n$ for some n. This means G is also a n-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$. Viewing two nontrivial elements of G as vectors, we know there is always an automorphism taking one vector to another, and so every nontrivial element is in the same orbit.

Every finite dimensional vector space over a field F is isomorphic to F^n for some n.

4. (January 2015 Problem 1) This problem concerns expressing groups as unions of proper subgroups.

(a) Show that no group is the union of two proper subgroups.

Suppose $G=H\cup K$. Note that $H\subseteq K \Rightarrow G=K$, so if H, K are proper subgroups, $H-K$ and $K-H$ must be nonempty. Let $x\in H-K$, $y\in K-H$. Then $xy\in G$, so $xy\in H$ or $xy\in K$. Without loss of generality, assume $xy\in H$. Then since $x\in H$, we must have $x^{-1}(xy)=y\in H$, a contradiction.

(b) Show that $\mathbb{Z}$ is not the union of any number of proper subgroups.

No proper subgroup of $\mathbb{Z}$ contains 1.

(c) For which n is $\mathbb{Z}^n$ the union of finitely many proper subgroups? What is the minimal number of such subgroups as a function of n?

For any $n>1$, $\mathbb{Z}^n$ is the union of 3 subgroups.

Let $A=\{(a_1,a_2,\ldots,a_n) \mid a_1+a_2 \text{ is even}\}$. This is a subgroup, since $(a_1+a_2)+(b_1+b_2)$ is even when a_1+a_2 and b_1+b_2 are even. Note that A contains all elements of $\mathbb{Z}^n$ where the first two coordinates are odd.

Let $B=\{(a_1,a_2,\ldots,a_n) \mid a_1 \text{ is even}\}$, $C=\{(a_1,a_2,\ldots,a_n) \mid a_2 \text{ is even}\}$. Then B and C are clearly subgroups, and they contain all elements with the first coordinate even, and the second coordinate even, respectively.

Then $\mathbb{Z}^n=A\cup B\cup C$.

Note that the key to this problem is recognizing that any set of subgroups of $\mathbb{Z}^2$ whose union is $\mathbb{Z}^2$ will give rise to subgroups of $\mathbb{Z}^n$ with the same property. One way to realize this is to consider the projection map $\mathbb{Z}^n\to\mathbb{Z}^2$. The pull back of a subgroup of $\mathbb{Z}^2$ is a subgroup of $\mathbb{Z}^n$, and any restriction of the subgroup of $\mathbb{Z}^2$ only applies to the first two coordinates in $\mathbb{Z}^n$.

5. (August 1996 Problem 1) We say that a group G has property (*) if every normal abelian subgroup of G is contained in its center.

(a) Suppose that N and M are normal subgroups of a group G and that G/N and G/M have property (*). Prove that $G/(N \cap M)$ has property (*).

Let $K \triangleleft G/N\cap M$ be a normal abelian subgroup. Let $x \in G/N\cap M$, and let $k \in K$. We want to show that $xk = kx$.

Consider the map $G/N\cap M \to G/M$, $x \mapsto \bar{x}$ ← This is the quotient map $(G/N\cap M)/(M/M\cap N)$

The image of K in this map is also normal and abelian. Since G/M has property (*), we know $\bar{x}\bar{k} = \bar{k}\bar{x}$. This means that $xk(kx)^{-1} \in M/(M\cap N)$. The same logic gives $xk(kx)^{-1} \in N/(M\cap N)$, and so $xk(kx)^{-1} = 1$, as desired.

(b) Let $N \triangleleft G$ and assume that G/N has property (*). If N has no non-trivial abelian normal subgroups, prove that G has property (*).

Let K be a normal abelian subgroup of G, and let $[K:G] = \{kgk^{-1}g^{-1} \mid k \in K, g \in G\}$. We want to show that $[K:G] = \{1\}$.

First note that $[K:G] \subseteq N$, since $kgk^{-1}g^{-1} = kg(gk)^{-1} \in N$ (by the same argument as part

Also, $[K:G] \subseteq K$, since $kgk^{-1}g^{-1} = k(gk^{-1}g^{-1}) \in K$ ($gk^{-1}g^{-1} \in K$ since K is normal).

Let L be the subgroup generated by $[K:G]$. Since $[K:G] \subseteq N\cap K$, we must have $L \subseteq N\cap K$. Since K is abelian, L is abelian.

We claim that L is also normal. We only need to show that $x[K:G] = [K:G]x$ for any $x \in G$. Let $x \in G$, $kgk^{-1}g^{-1} \in [K:G]$. Since $k \in K$, there is $\ell \in K$ with $k = x^{-1}\ell x$. We have

$$x(kgk^{-1}g^{-1}) = x(x^{-1}\ell x)g(x^{-1}\ell x)^{-1}g^{-1} = \ell x g x^{-1}\ell^{-1}xg^{-1} = \ell(xgx^{-1})\ell^{-1}(xg^{-1}x^{-1})x = \ell(xgx^{-1})\ell^{-1}(xgx^{-1})^{-1}x$$

Thus L is abelian, normal, and contained in N, which implies L is trivial, which finishes the proof.

(c) Show that a finite p-group with property (*) must be abelian.

Suppose G is such a group which is not abelian. Then $G/Z(G)$ is a nontrivial p-group, which has nontrivial center (because it is a p-group). Let $a \in Z(G/Z(G))$, and consider the cyclic subgroup of $G/Z(G)$ generated by a. This subgroup lifts to a subgroup $H \subseteq G$, which is normal (since its image is in the center).

Let $x, y \in H$. Then under the map $G \to G/Z(G)$, we have $x \mapsto a^m$, $y \mapsto a^n$ for some m, n. Thus $x^{-1}a^m$, $y^{-1}a^n \in Z(G)$, and so there are $b, c \in Z(G)$ with $x = a^m b$, $y = a^n c$. We have

$$xy = a^m b a^n c = a^n c a^m b = yx.$$

Thus H is an abelian normal subgroup which is not contained in $Z(G)$, a contradiction.

1. (January 2013 Problem 1) A finite group G is said to have property C if, whenever $g \in G$ and n is an integer relatively prime to the order of G, g and g^n are conjugate in G.

(a) Give infinitely many non-isomorphic finite groups which have property C.

Claim: S_n has property C.

Theorem: Two permutations are conjugate iff they have the same cycle structure.

proof:
Since every permutation is the product of disjoint cycles, it suffices to check that property holds for cycles $g \in G$.

Let m be relatively prime to $|S_n| = n!$ and let $g = (1\ 2 \cdots r)$ be a cycle in S_n.

Now g^m is the permutation:

$$\begin{aligned} 1 &\longmapsto 1+m \pmod r \\ 1+m &\mapsto 1+2m \pmod r \\ &\vdots \qquad\quad \vdots \end{aligned}$$

So it suffices to check that each $1+im \pmod r$ is distinct for $i = 1, \ldots, r$.

Note: $1+im \equiv 1+jm \pmod r \iff (i-j)m$ is divisible by r.
→ Since $\gcd(m,r) = 1$, this gives $r \mid (i-j)$, so $i \equiv j \bmod r$.

$\gcd(m, n!) = 1$, and $r \mid n!$

Thus we have shown that S_n has property C for all $n \in \mathbb{N}$

Alternative Solution:
$\mathbb{Z}/2\mathbb{Z}$ has property C, and it is easy to check that the direct product of two groups with property C will also have property C. Thus $(\mathbb{Z}/2\mathbb{Z})^n$ has property C for $n \in \mathbb{N}$.

(b) Give infinitely many non-isomorphic finite groups which do not have property C.

$\mathbb{Z}/n\mathbb{Z}$ does not have property C for $n > 2$

A generator raised to a relatively prime power is a distinct element, which is certainly not in the same conjugacy class since $\mathbb{Z}/n\mathbb{Z}$ is abelian.

(c) Show that if G has property C and $\rho : G \to GL_n(\mathbb{C})$ is a homomorphism, then the trace of $\rho(g)$ is in $\mathbb{Q}$ for all $g \in G$.

Claim 1: The eigenvalues of $\rho(g)$ are $|G|$-roots of unity (for any $g \in G$)

~~Proof~~:
$\rho(g)^{|G|} = \rho(g^{|G|}) = \rho(1) = 1.$

$\rho(g)$ is a matrix whose $|G|^{th}$-power is I_n.

If ξ is an eigenvalue of $\rho(g)$, then $\xi^{|G|} = 1$.
So ξ is a $|G|$-root of unity.

If ξ is an eigenvalue of $\rho(g)$, then $\xi^{|G|}$ is an eigenvalue of I_n

Note (Representation Theory):
This question essentially says that if a group has property C, then the character table is rational. It is classically known that S_n has a rational character table.

Claim 2: Let ξ be a $|G|$-root of unity. Then $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ is the maps $\xi \mapsto \xi^m$ where m is relatively prime to $|G|$.

~~proof~~.
Any $\sigma \in Gal(\mathbb{Q}(\xi)/\mathbb{Q})$ must send ξ to another primitive root, i.e. to a relatively prime power.

Conversely, all primitive roots are roots of the same irreducible polynomial. The Galois extension property implies the claim.

Galois Extension Property
There exists an automorphism which sending any root of an irreducible polynomial to any other root

Claim 3: If G has property C, then $tr(\rho(g)) \in \mathbb{Q}$ for each $g \in G$.

~~proof~~:
Let $g \in G$, m relatively prime to $|G|$.

Trace is invariant under conjugation

We have $tr(\rho(g)) = \sum_j \xi^j = tr(\rho(g^m))$

Now if $\sigma \in Gal(\mathbb{Q}(\xi)/\mathbb{Q})$, $\sigma : \xi \mapsto \xi^m$, we have

$$tr(\rho(g^m)) = \sum_j (\xi^m)^j = \sum_j \sigma(\xi^m) = \sigma\left(\sum_j \xi^j\right) = \sigma(tr(\rho(g)))$$

Thus we have shown that $tr(\rho(g))$ is fixed by every element of $Gal(\mathbb{Q}(\xi)/\mathbb{Q})$, which implies $tr(\rho(g)) \in \mathbb{Q}$.

Note: We have shown that the trace is the sum of roots of unity, which are algebraic integers, and the only algebraic integers in $\mathbb{Q}$ are the integers, so we have actually shown that $tr(\rho(g)) \in \mathbb{Z}$.

2. (August 2014 Problem 3) Let G be a finite group.

(a) If H is a proper subgroup of G, show that there is some element $x \in G$ which is not contained in any subgroup conjugate to H.

Suppose not. Then $G = \bigcup_g gHg^{-1}$, and so

$|G| < (\#\text{ of conjugates of } H) \cdot |H|$

(Each conjugate has size $|H|$, but they are not disjoint, so strict inequality)

Thus we get

$$|G| < [G : N_G(H)] \cdot |H| = \frac{|G|}{|N_G(H)|} \cdot |H|$$

$$\Rightarrow |N_G(H)| < |H|.$$

This is a contradiction, since $H \leq N_G(H)$.

Fact: A subgroup H of a finite group G has $[G : N_G(H)]$ conjugate subgroups.

proof

G acts on the set of subgroups by conjugation. The orbit-stabilizer theorem gives

$$|G| = |\text{Stab}(H)| \cdot |\text{Orb}(H)|$$

for a subgroup $H \leq G$. $\text{Orb}(H)$ under the action is the set of subgroups conjugate to H. $\text{Stab}(H)$ is the set $\{g \in G : gHg^{-1} = H\} = N_G(H)$. Thus we get

$$|G| = |N_G(H)| \cdot (\#\text{ of subgroups conjugate to } H).$$

(b) A *maximal subgroup* of G is a proper subgroup which is not contained in any other proper subgroup. Derive from the first part of the problem that if all maximal subgroups of G are conjugate, G must be cyclic.

Since every maximal subgroup is conjugate, by part (a), we know there is some $x \in G$ which is not contained in any maximal subgroup.

We will show that $\langle x \rangle = G$.
Suppose $\langle x \rangle \neq G$, and let X be the set of proper subgroups H such that $\langle x \rangle \leq H$.
X is nonempty, since $\langle x \rangle \in X$.

Let $H_1 \leq H_2 \leq \cdots$ be a chain of subgroups of G.
Since G is finite, this chain must stabilize.
At this point, we have achieved an upper bound.
By Zorn's Lemma, X has a maximal element, H.
But $x \in H$, contradiction.

Zorn's Lemma
If a partially ordered set has the property that every chain has an upper bound, then the set has a maximal element.

3. (January 1991 Problem 5) Let G be a possibly infinite, non-trivial group whose subgroups are linearly ordered by inclusion. In other words, if H and K are subgroups of G, then either $H \subseteq K$ or $K \subseteq H$.

   (a) Prove that G is an abelian group, and that the orders of the elements of G are all powers of the same prime p.

Claim: G is abelian.

proof

Let $x, y \in G$. Then either $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle$. Then either $x = y^n$ or $y = x^n$ for some n, and so x and y commute.

Claim Each element of G has finite order.

proof

If $\langle x \rangle$ has infinite order, then $\langle x^2 \rangle \not\subseteq \langle x^3 \rangle$ and $\langle x^3 \rangle \not\subseteq \langle x^2 \rangle$. Contradiction.

Claim: Every element has the same prime-power order.

proof

Let p, q be primes which divide the order of $\langle x \rangle$. By Cauchy's theorem, $\langle x \rangle$ has subgroups of order p and q. If $p \neq q$, these subgroups cannot contain one another. So the order of x is p^k for some k

Now suppose x has order p^k and y has order p^n. Then we apply Cauchy's theorem again to obtain subgroups of order p and q, so $p = q$.