110AH Final Review Problem Solutions

Colin Ni

December 10, 2023

Star means highly recommended.

Problem 1*. Let $n \geq 3$. Construct an injection $D_{2n} \hookrightarrow S_n$. Prove or disprove: S_n is the smallest symmetric group into which D_{2n} embeds.

Solution. The idea is as follows. Recall that D_{2n} is the group of rigid symmetries of a regular n-gon, whereas S_n is the group of symmetries of the n numbers $1, \dots, n$. Thus, thinking of the numbers $1, \dots, n$ as labeling the n vertices of a regular n-gon, the elements of D_{2n} (injectively) become elements of S_n.

More precisely, recall that

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle,$$

so the homomorphisms from D_{2n} to any group G are given by

$$\operatorname{Hom}(D_{2n}, G) = \{(u, v) \in G \mid u^n = v^2 = 1, uv = vu^{-1}\};$$

spelling it out, a homomorphism $\varphi\colon D_{2n} \to G$ corresponds to $(\varphi(r), \varphi(s))$, and (u, v) corresponds to the homomorphism φ taking $u \mapsto r$ and $v \mapsto s$ (which exists by the universal property of quotients). Consider the elements

$$u = (1\ 2\ \cdots\ n) \qquad \text{and} \qquad v = \begin{cases} (1\ n)(2\ n-1)\cdots(\frac{n}{2}-1\ \frac{n}{2}) & n \text{ even} \\ (2\ n)(3\ n-1)\cdots(\frac{n-1}{2}\ \frac{n+1}{2}) & n \text{ odd} \end{cases}$$

of S_n. Certainly $u^n = v^2 = 1$ and

$$vu^{-1}v = (v(n)\ v(n-1)\ \cdots\ v(2)\ v(1)) = \begin{cases} (1\ 2\ \cdots\ n-1\ n) & n \text{ even} \\ (2\ 3\ \cdots\ n\ 1) & n \text{ odd} \end{cases} = u,$$

so there is a map $\varphi\colon D_{2n} \to S_n$ taking $r \mapsto u$ and $s \mapsto v$.

Let us show φ is injective by showing that no nonidentity element of D_{2n} is in the kernel. Since $\varphi(r)$ has order n, the elements $r, \dots, r^{n-1}$ are not in the kernel, and similarly since $\varphi(s)$ has order 2, the element s is not either. It remains to see that the remaining elements $sr, \dots, sr^{n-1}$ are not in the kernel. For n even, when $0 < k < n-1$ the permutation $\varphi(sr^k)$ takes 1 to $n-k$, and the permutation $\varphi(sr^{n-1})$ takes 2 to n. For n odd, when $0 < k < n$ the permutation $\varphi(sr^k)$ takes 1 to $n-k+1$.

It is not true that S_n is the smallest symmetric group into which D_{2n}. For example, $D_{12} \hookrightarrow S_5$ via the map $r \mapsto (1\ 2)(3\ 4\ 5)$ and $s \mapsto (1\ 2)(3\ 4)$. It is easy to check that this satisfies the above relations and that the induced homomorphism is injective. □

Problem 2*. Let A and B be abelian groups. Denote by $\operatorname{Hom}(A, B)$ the set of group homomorphisms $A \to B$.

(a) Explain how $\operatorname{Hom}(A, B)$ is naturally an abelian group.

(b) Describe $\operatorname{Hom}(\mathbb{Z}, B)$ and $\operatorname{Hom}(C_n, B)$.

(c) In particular, for A and B cyclic, compute $\operatorname{Hom}(A, B)$.

Solution. For (a), use point-wise addition. More precisely, given $f, g \in \operatorname{Hom}(A, B)$, define $f + g$ via

$$(f + g)(a) = f(a) + g(a).$$

This makes $\operatorname{Hom}(A, B)$ an abelian group since associativity and abelian-ness come from associativity and abelian-ness of the operation in B, the identity is the constant homomorphism at 0, and the inverse of f is the homomorphism $-f$ defined by $(-f)(a) = -f(a)$.

For (b), we have

$$\operatorname{Hom}(\mathbb{Z}, B) = B \qquad \text{and} \qquad \operatorname{Hom}(C_n, B) = B[n],$$

where $B[n] = \{a \in A \mid na = 0\}$ denotes the n-torsion in B. Indeed, maps from $\mathbb{Z}$ and C_n are determined by the image of 1, and for $\mathbb{Z}$ this image can be any element whereas for C_n this image must be an n-torsion element.

For (c), the answer is

$$\operatorname{Hom}(A, B) = \begin{cases} B & A = \mathbb{Z} \\ C_{\gcd(m,n)} & A = C_m \text{ and } B = C_n \\ 0 & A = C_m \text{ and } B = \mathbb{Z}. \end{cases}$$

Indeed the first and third cases follow almost immediately from part (b), and the second case is the computation

$$C_n[m] = \ker(\times m \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}) = \left(\frac{n}{\gcd(m, n)}\mathbb{Z}\right)/(n\mathbb{Z}) \cong C_{\gcd(m,n)}. \quad \square$$

Remark. The construction in (a) does not work in general when B is nonabelian since fg may not be a homomorphism. It does however make $\operatorname{Hom}(A, B)$ a groupoid by restricting to the products that become homomorphisms.

Problem 3*. A theorem of Gauss says that $(\mathbb{Z}/n\mathbb{Z})^\times$, where $n \geq 1$, is cyclic if and only if n is 1, 2, 4, or p^k or $2p^k$ for some odd prime p and $k > 0$. Use this to help fill out the following table of information about $(\mathbb{Z}/n\mathbb{Z})^\times$:

n	cyclic	order	structure	gens	# gens	min size gen set
3						
4						
5						
6						
7	yes	6	C_6	$1, 5$	2	1 (e.g. $\{5\}$)
8	no	4	$C_2 \times C_2$	0	none	2 (e.g. $\{3, 5\}$)
9						
10						
11						
12						
24						
122						
1125						
7938						

Solution. The filled out table is as follows:

n	cyclic	order	structure	# gens	gens	min size gen set
3	yes	2	C_2	1	2	1
4	yes	2	C_2	1	3	1
5	yes	4	C_4	2	$2, 3$	1
6	yes	2	C_2	1	5	1
7	yes	6	C_6	2	$3, 5$	1 (e.g. $\{5\}$)
8	no	4	$C_2 \times C_2$	0	none	2 (e.g. $\{3, 5\}$)
9	yes	6	C_6	2	$2, 5$	1
10	yes	4	C_4	2	$7, 8$	1
11	yes	10	C_{10}	4	$2, 6, 7, 8$	1
12	no	4	$C_2 \times C_2$	0	none	2
24	no	8	$C_2 \times C_2 \times C_2$	0	none	3
122	yes	60	C_{60}	16	below	1
1125	no	600	$C_6 \times C_{100}$	0	none	2
7938	no	2268	$C_{54} \times C_{42}$	0	none	2

Note that

$$122 = 2 \cdot 61, \qquad 1125 = 3^2 \cdot 5^3, \qquad \text{and} \qquad 7938 = 2 \cdot 3^4 \cdot 7^2.$$

Whether $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic is determined by the described theorem of Gauss. The order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is given by $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$, where φ denotes the Euler totient function which can be easily computed using the prime factorization of n.

Now we determine the structure of the non-cyclic cases. Of course $(\mathbb{Z}/8\mathbb{Z})^\times$ and $(\mathbb{Z}/12\mathbb{Z})^\times$ are $C_2 \times C_2$ since they are order 4 but not cyclic. In general, if

n has canonical prime factorization $p_1^{k_1} \cdots p_n^{k_n}$, then

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_n^{k_n}\mathbb{Z})^\times$$

by the Chinese remainder theorem and the general fact that the units in a direct product of rings is the direct product of the units. Thus, again using the described theorem of Gauss, we have

$$(\mathbb{Z}/24\mathbb{Z})^\times = (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times = C_2 \times C_2 \times C_2,$$

$$(\mathbb{Z}/1125\mathbb{Z})^\times = (\mathbb{Z}/9\mathbb{Z})^\times \times (\mathbb{Z}/125\mathbb{Z})^\times = C_6 \times C_{100},$$

and

$$(\mathbb{Z}/7938\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3^4\mathbb{Z})^\times \times (\mathbb{Z}/7^2\mathbb{Z})^\times = C_{54} \times C_{42}.$$

The number of generators of a noncyclic group is 0, and the number of generators of C_k is again $|(\mathbb{Z}/k\mathbb{Z})^\times| = \varphi(k)$. To find generators for the smaller cases, just compute by hand, and for the case $n = 122$, use the following line of Python:

```
>>> sorted([
...     k
...     for k in range(122)
...     if len({(k ** n) % 122 for n in range(122)}) == 60
...])
[7, 17, 31, 35, 43, 51, 55, 59, 63, 67, 71, 79, 87, 91, 105, 115]
```

Finally, the minimal size of a generating set is 1 in the cyclic case and at most the number of factors of the structure in the noncyclic case. That $C_2 \times C_2 \times C_2$ cannot be generated by two elements is implied by Problem 8 on HW 5. $\square$

Problem 4*. Find the smallest $n \geq 1$ where S_n has an element of order $5n$.

Solution. We will show more generally that S_n has an element of order $k = p_1^{e_1} \cdots p_k^{e_k}$ if and only if

$$n \geq p_1^{e_1} + \cdots + p_k^{e_k}.$$

Recall that the order of any $\sigma \in S_n$ is $\operatorname{lcm}(\ell_1, \ldots, \ell_m)$, where $\ell_1, \ldots, \ell_m$ are the lengths of the cycles in the disjoint cycle decomposition of σ. So the reverse direction is clear. Conversely, consider a $\sigma \in S_n$ with order k that has minimal length $\ell_1 + \cdots + \ell_m$, which exists due to the hypothesis. Having minimal length forces the ℓ_i to be pairwise coprime since the order of σ is given by their lcm. It also forces each ℓ_i to be a prime-power since $ab > a + b$ whenever $a, b \geq 2$ are distinct. Thus the ℓ_i are precisely the prime powers in the prime factorization of k.

Therefore the following table shows that for $n < 12$, there does not exist an element of order $5n$ in S_n.

n	$5n$	$p_1^{e_1},\ldots,p_k^{e_k}$	$p_1^{e_1}+\cdots+p_k^{e_k}$
1	5	5	5
2	10	2, 5	7
3	15	3, 5	8
4	20	4, 5	9
5	25	25	25
6	30	2, 3, 5	11
7	35	5, 7	12
8	40	8, 5	13
9	45	9, 5	14
10	50	2, 25	27
11	55	5, 11	16
12	60	4, 3, 5	12

For $n = 12$, there indeed exists an element of order 60, e.g.

$$(1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9\ 10\ 11\ 12). \qquad \square$$

Problem 5. Let p be an odd prime. Show that the only groups of order $2p$ are C_{2p} and D_{2p}.

Problem 6. Is the following 4×4 sliding tile puzzle solvable?:

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Solution. No, roughly speaking because the sign of the permutation plus the manhattan distance of the blank square is an invariant.

More precisely, consider any sequence of positions $\sigma_1, \sigma_2, \ldots$ resulting from valid moves, where σ_1 is the starting position. Think of the blank square as 16 so that any position σ_k is an element of S_{16}, for example $\sigma_0 = (14\ 15)$. Given a position σ_k, a move corresponds to swapping 16 with a vertically or horizontally adjacent number a_k, or in other words it multiplies the current position by a transposition via $\sigma_{k+1} = \sigma_k(a_k\ 16)$. A move also increases or decreases the manhattan distance d_k between 16 and the bottom-right corner by exactly 1. Denote by $\operatorname{asgn}(\sigma_k) \in \{0, 1\}$ the additive sign of σ_k. Then by our above observations

$$\operatorname{asgn}(\sigma_k) + d_k \equiv 1 \mod 2$$

for all k, so the puzzle cannot be solved because the solved position σ is such that

$$\operatorname{asgn}(\sigma) + d = \operatorname{asgn}(1) + 0 = 0. \qquad \square$$

Problem 7*.

(*a*) Show that every dihedral group has an index 2 subgroup, and generalize this to exhibit an infinite nonabelian group that has an index 2 subgroup.

(*b*) Denote by S_∞ the group of permutations of $\mathbb{N}$, where $S_n \hookrightarrow S_\infty$ in the natural way. A theorem of Schreier-Ulam says that the only proper nontrivial normal subgroups of S_∞ are $\bigcup_{n\geq 1} S_n$ and $\bigcup_{n\geq 1} A_n$. Use this to show that S_∞ does not have an index 2 subgroup.

(*c*) (Optional) Show that the only groups whose proper nontrivial subgroups all have index 2 are the simple cyclic groups, C_4, and $C_2 \times C_2$.

Solution. For (*a*), the easy argument is that the subgroup $\langle r\rangle$ has order n, hence is an index 2 subgroup. However, here is an argument more suited to the infinite case. Intuitively, consider the homomorphism po that detects whether a symmetry in D_{2n} of the regular n-gon preserves the orientation of the regular n-gon, i.e. whether it contains an s. More precisely, consider the induced homomorphism

$$\begin{aligned} \mathrm{po}\colon D_{2n} &\longrightarrow \{-1,+1\} \\ r &\longmapsto 1 \\ s &\longmapsto -1, \end{aligned}$$

which exists because (see solution to Problem 1)

$$\mathrm{po}(r^n) = \mathrm{po}(s^2) = 1 \qquad \text{and} \qquad \mathrm{po}(sr) = -1 = \mathrm{po}(r^{-1}s).$$

Since $\ker \mathrm{po} = \langle r\rangle$, by the first isomorphism theorem $\langle r\rangle$ has index 2.

The infinite case is now clear. Consider the subgroup $D \leq \mathrm{GL}_2(\mathbb{R})$ generated by a flip and the rotations, i.e.

$$s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{and} \qquad r_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for } \theta \in [0, 2\pi).$$

Note that $sr_\theta = r_\theta^{-1}s$ and $r_\theta^{-1} = r_{-\theta}$, so any element of D can be written uniquely as $s^a r_\theta$ for some $a \in \{0,1\}$ and $\theta \in [0,2\pi)$. Again

$$\begin{aligned} \mathrm{po}\colon D &\longrightarrow \{-1,+1\} \\ r_\theta &\longmapsto 1 \\ s &\longmapsto -1 \end{aligned}$$

induces a homomorphism $D \to \{-1,+1\}$ since

$$\begin{aligned} \mathrm{po}(s^a r_\theta s^{a'} r_{\theta'}) &= \mathrm{po}(s^{a+a'} r_{\theta'-\theta}) \\ &= (-1)^{a+a'} = (-1)^a(-1)^{a'} \\ &= \mathrm{po}(s^a r_\theta)\mathrm{po}(s^{a'} r_{\theta'}). \end{aligned}$$

For (b), recall that any subgroup of index 2 is normal by Problem 6 on Homework 5, so it suffices to show that both normal subgroups of S_∞ have index greater than 2. Moreover, since $\bigcup_{n\geq 1} A_n \leq \bigcup_{n\geq 1} S_n$, it suffices to show this for the latter.

In fact, we will show that $\bigcup_{n\geq 1} S_n$ has infinite index in S_∞. Let $k \geq 2$, and consider the element $\sigma_k \in S_\infty$ defined roughly by

$$\sigma_k = (1 \ \cdots \ k)(k+1 \ \cdots \ 2k)\cdots$$

or more precisely as the bijection $\sigma_k \colon \mathbb{N} \to \mathbb{N}$ defined by

$$\sigma_k(a) = \begin{cases} a+1 & a \not\equiv k-1 \mod k \\ a-(k-1) & a \equiv k-1 \mod k. \end{cases}$$

Certainly σ_k has order k in $S_\infty / \bigcup_{n\geq 1} S_n$ (in fact also in S_∞) since $\sigma_k, \ldots, \sigma_k^{k-1}$ all move an infinite number of elements and since $\sigma_k^k = 1$. Thus k divides the order of $S_\infty / \bigcup_{n\geq 1} S_n$, i.e. the index of $\bigcup_{n\geq 1} S_n$. Since $k \geq 2$ was arbitrary, this index is infinite.

For (c), it is clear that the simple cyclic groups, C_4, and $C_2 \times C_2$ satisfy the criteria. Conversely, let G be a group whose proper nontrivial subgroups all have index 2.

Suppose for the sake of contradiction that G is infinite. Let $1 \lneq H \lneq G$ be a proper nontrivial subgroup, and pick a nonidentity element $x \in H$ so that $1 \lneq \langle x \rangle \leq H \lneq G$. Observe that

$$2[H : \langle x \rangle] = [G : H][H : \langle x \rangle] = [G : \langle x \rangle] = 2.$$

This shows $[H : \langle x \rangle] = 1$, so $H = \langle x \rangle$. The generator x of this cyclic subgroup must have infinite order since H is an index 2 subgroup in an infinite group, so

$$[G : \langle x^2 \rangle] = [G : \langle x \rangle][\langle x \rangle : \langle x^2 \rangle] = 4,$$

a contradiction. Thus G is finite.

Now let us show that G is simple cyclic, C_4, or $C_2 \times C_2$. Suppose G is not simple cyclic, i.e. $|G|$ is not prime. Let p be a prime dividing $|G|$ so that Cauchy's theorem produces an element $x \in G$ of order p. Since $\langle x \rangle$ has index 2, already $|G| = 2p$. Thus the first Sylow theorem ensures G has a nontrivial Sylow-2 subgroup P, but P cannot be proper because then it would have index 2, contrary to P being Sylow. Hence $G = P$, i.e. $p = 2$ and $|G| = 4$. We conclude that G is C_4 or $C_2 \times C_2$. □

Remark. For (a), note that the subgroup of $\mathrm{GL}_2(\mathbb{R})$ constructed in the solution is not the so-called *infinite dihedral group*, which is defined as $\langle r, s \mid s^1 = 1, rs = sr^{-1} \rangle$. Indeed the infinite dihedral group is countable, whereas the subgroup in the solution is uncountable. Instead, what we have constructed is the orthogonal group and the special orthogonal group $\mathrm{SO}_2(R) \leq \mathrm{O}_2(R)$.

Problem 8. Prove, or disprove and find a minimal counterexample:

- If G is a finite group and $d \mid |G|$, then G has an element of order d.
- If G is a finite group and $d \mid |G|$, then G has a subgroup of order d.

You may use that the list of non-abelian groups in increasing order starts with $D_6, D_8, Q_8, D_{10}, D_{12}, A_4, \dots$.

Solution. Certainly the first statement is true for the groups $1, C_2, C_3$ of order at most 3. However, it is not true for $C_2 \times C_2$ since this group does not have an element of order 4, so this is a minimal counterexample.

For the second statement, note it is true for finite abelian groups, which are products of prime-power order cyclic groups, for example

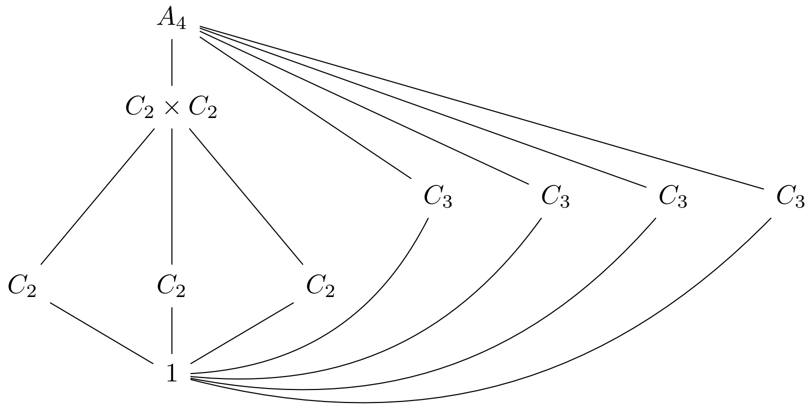
$$\langle (2^0,0,0,0),(0,2^3,0,0),(0,0,5^0,0),(0,0,0,5^3)\rangle \leq \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^3\mathbb{Z}} \times \frac{\mathbb{Z}}{5^{13}\mathbb{Z}} \times \frac{\mathbb{Z}}{5^{17}\mathbb{Z}}$$

has order $2^{2-0} \cdot 2^{3-3} \cdot 5^{13-0} \cdot 5^{17-3} = 2^2 \cdot 5^{27}$. It therefore suffices to consider the non-abelian groups. The statement is true for the nonabelian groups up to D_{12} in the list, since the following subgroups have orders that cover all the proper divisors:

$$\langle s\rangle, \langle r\rangle \leq D_6$$
$$\langle s\rangle, \langle r\rangle \leq D_8$$
$$\langle -1\rangle, \langle i\rangle \leq Q_8$$
$$\langle s\rangle, \langle r\rangle \leq D_{10}$$
$$\langle s\rangle, \langle r^3\rangle, \langle r^2\rangle, \langle r\rangle \leq D_{12}.$$

However, A_4 does not have a subgroup of order 6 by Problem 10 on Homework 7 (see remark below for a solution), so this is a minimal counterexample. □

Remark. Here is a solution to Problem 10 on Homework 7, which asks you to prove that A_4 does not have a subgroup of order 6. In fact we will prove that the subgroup lattice of A_4 is as follows, where as usual the subgroups are collected by level according to their orders:



Indeed, the subgroups of order 2 are

$$\langle(1\ 2)(3\ 4)\rangle, \langle(1\ 3)(2\ 4)\rangle, \langle(1\ 4)(2\ 3)\rangle$$

since every such subgroup is cyclic and since these subgroups are pairwise distinct and contain all order 2 elements in A_4. Similarly, the subgroups of order 3 are

$$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle.$$

There is only one subgroup of order 4, namely $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$, by the following argument. Any such subgroup is isomorphic to C_4 or $C_2 \times C_2$. Certainly there are no elements of order 4 in A_4 (in particular, 4-cycles are not even), so there is no copy of C_4. The subgroup $\langle(1\ 2)(3\ 4), (1\ 3)(2\ 4)\rangle$ is a copy of $C_2 \times C_2$, and it contains all three copies of C_2 in A_4. Moreover it is the only copy of $C_2 \times C_2$ in A_4 because any such copy must contain 3 copies of C_2 in A_4, of which there are only 3.

Finally, there are no subgroups of order 6 in A_4 by the following argument. Any such subgroup is isomorphic to $C_2 \times C_3$ or D_6. The former would be abelian and generated by an order 2 element and an order 3 element, but it is easy to argue that no element of order 2 in A_4 (i.e. a double transposition) commutes with an element of order 3 in A_4 (i.e. a 3-cycle). Similarly, the latter would be generated by an order 2 element s and an order 3 element r in A_4 such that $r = sr^{-1}s^{-1}$, but this does not work in A_4 because every order 2 element conjugates a copy of C_3 to a different copy of C_3, e.g. $(1\ 3)(2\ 4)$ conjugates $\langle(1\ 2\ 4)\rangle$ to $\langle(2\ 3\ 4)\rangle$.

Problem 9*.

(*a*) Show that if $S \subset G$ is a normal subset of a group, i.e. $gSg^{-1} \subset S$ for all $g \in G$, then $\langle S\rangle$ is normal.

(*b*) Show that $A_{3 \cdot 5^2 \cdot 19}$ is generated by the permutations of the form

$$(a_1\ a_2\ a_3)(b_1\ b_2\ b_3\ b_4\ b_5)(c_1\ c_2\ c_3\ c_4\ c_5)(d_1\ d_2\ \cdots\ d_{18}\ d_{19})$$

where the a_i, b_i, c_i, d_i are pairwise distinct.

(*c*) Show that a nontrivial simple group is generated by its elements of order p if and only if contains an element of order p.

Solution. For (*a*), this is Problem 1 on Homework 6. Here is a solution (also on Bruinlearn) for reference. To show that $\langle S\rangle \trianglelefteq G$, we will show that $c_g(s) \in \langle S\rangle$ for any $s \in \langle S\rangle$ and $g \in G$, where c_g denotes conjugation by g. Writing $s = s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}$ for some $s_i \in S$ and $\epsilon \in \{-1, +1\}$, compute

$$c_g(s_1^{\epsilon_1} \cdots s_n^{\epsilon_n}) = c_g(s_1)^{\epsilon_1} \cdots c_g(s_n)^{\epsilon_n}$$

using that c_g is a homomorphism. Since $c_g(s_i) \in S$ by assumption, the RHS is in $\langle S\rangle$.

For (b), first note that the problem statement contains several red herrings. More generally, let $n \geq 5$, fix a nontrivial even cycle type (i.e. one for which there exists a nontrivial element of A_5 with that cycle type), and consider the subgroup $\langle S \rangle$ generated by the set S of permutations of that cycle type. Since conjugation preserves cycle type, we have $\sigma S \sigma^{-1} \subset S$ for any $\sigma \in A_n$. Thus by part (a), the subgroup $\langle S \rangle$ is normal, and since our cycle type was nontrivial, so too is $\langle S \rangle$. It follows that $\langle S \rangle = A_n$ by simplicity of A_n, using that $n \geq 5$.

For (c), let G be a nontrivial simple group. The forward direction is immediate because G is nontrivial. Conversely, suppose $x \in G$ has order p, and consider $S = \{gxg^{-1} \mid g \in G\}$. Since conjugation preserves order of elements, S consists of elements of order p, so it suffices to show that $\langle S \rangle = G$. But $gSg^{-1} \subset S$ by construction, so $\langle S \rangle$ is normal in G by part (a) and nontrivial because $x \in S$. By simplicity of G, we have $\langle S \rangle = G$, as desired. □

Problem 10. A group G is said to be k-abelian if $(ab)^k = a^k b^k$ for every $a, b \in G$. Show that if a group G is k-, $(k+1)$-, and $(k+2)$-abelian for some $k \in \mathbb{Z}$, then G is abelian.

Solution. Let G be a group that is k-, $(k+1)$-, and $(k+2)$-abelian for some $k \in \mathbb{Z}$. Take $a, b \in G$. Then b commutes with a^k and a^{k+1} since

$$a^{k+1}b^{k+1} = (ab)^{k+1} = (ab)(ab)^k = aba^k b^k$$

implies $a^k b = ba^k$ and similarly

$$a^{k+2}b^{k+2} = (ab)^{k+2} = (ab)(ab)^{k+1} = aba^{k+1}b^{k+1}$$

implies $a^{k+1}b = ba^{k+1}$. Therefore

$$ab = aba^k a^{-k} = a^{k+1}ba^{-k} = ba.$$ □

Problem 11. Let p be an odd prime. The *Legendre symbol* $\left(\frac{-}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a square in } (\mathbb{Z}/p\mathbb{Z})^* \\ -1 & a \text{ is not a square in } (\mathbb{Z}/p\mathbb{Z})^*. \end{cases}$$

Prove that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$.

Problem 12*. Let $G \leq \mathbb{C}^*$ the group of p-power roots of unity, where p is a fixed prime. Show that there exists a nontrivial $N \trianglelefteq G$ such that $G \cong G/N$

Solution. Write

$$G = \left\{ \exp\left(i\frac{2k\pi}{p^n}\right) \;\middle|\; n \geq 0, k \in \mathbb{Z} \right\},$$

and consider the surjective homomorphism

$$\begin{aligned} \varphi \colon G &\longrightarrow G \\ \xi &\longmapsto \xi^p \end{aligned}$$

with nontrivial $\ker\varphi \ni \exp\left(i\frac{2\pi}{p}\right) \neq 1$. The first isomorphism theorem gives the result. □

Problem 13. For which n, m can S_n be embedded into A_m?

Solution. From Midterm II, for which solutions are available on Bruinlearn, for any n we have $S_n \leq A_{n+2}$, so

$$S_n \leq A_m \qquad \text{for} \qquad m \geq n+2.$$

Certainly

$$S_n \not\leq A_m \qquad \text{for} \qquad 2 \leq m \leq n$$

since in this case $|A_m| = m!/2 < n! = |S_n|$.

For the case $m = n+1$, we will show that S_n cannot be properly embedded into A_{n+1} for any n. Suppose $S_n \leq A_{n+1}$ for some n. (We will show that $n = 1$, whence the embedding is not proper.) This induces the usual nontrivial homomorphism

$$A_{n+1} \to S_{[A_{n+1}:S_n]} = S_{\frac{n+1}{2}}$$

induced by the action of A_{n+1} on the cosets of S_n by left-multiplication. Note that n is odd in order for $(n+1)/2$ to even be an integer. Moreover, $n < 4$ since if $n+1 \geq 5$, then the kernel must be trivial because it is proper whereas A_{n+1} is simple, but

$$(n+1)!/2 = |A_{n+1}| \leq |S_{(n+1)/2} = ((n+1)/2)!$$

is absurd for $n = 5$ and even more absurd for $n = 7, 9, \ldots$ (this is induction). Thus $n < 4$, so $n \in \{1, 3\}$. But A_{3+1} has no subgroup of order 6 by Problem 10 on Homework 7 (see also remark after Problem 8) and hence has no subgroup isomorphic to S_3, so $n = 1$. □

Problem 14*. A group G is *finitely generated* if there exists a finite set $S \subset G$ such that $G = \langle S \rangle$. Obviously finite groups are finitely generated, so let us examine infinite groups.

(a) Show that $\mathbb{Z}^n$ is finitely generated.

(b) Show that $\mathbb{Q}$ is not finitely generated because its finitely generated subgroups are cyclic.

(c) Show that $\mathbb{R}$ is not finitely generated but that it has finitely generated subgroups that are not cyclic.

(d) Show that the finitely generated group $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \leq \mathrm{GL}_2(\mathbb{Q})$ has a subgroup that is not finitely generated, namely the one consisting of the matrices in the group with ones on the diagonal.

Remark. A theorem of Higman, Neumann, and Neumann says that every countable group can be embedded into a group generated by two elements.

Solution. For (a), write

$$\mathbb{Z}^n = \{a_1e_1 + \cdots + a_ne_n \mid a_1, \ldots, a_n \in \mathbb{Z}\} = \langle e_1, \ldots, e_n \rangle.$$

For (b), note that for any $r_1/s_1, \ldots, r_n/s_n \in \mathbb{Q}$ we have

$$\langle r_1/s_1, \ldots, r_n/s_n \rangle \leq \langle 1/(s_1 \cdots s_n) \rangle,$$

so the subgroup generated by these elements is cyclic because subgroups of cyclic groups are cyclic. This shows that $\mathbb{Q}$ is not finitely generated because $\mathbb{Q}$ is obviously not cyclic.

For (c), observe that

$$\langle x_1, \ldots, x_n \rangle = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in \mathbb{Z}\}$$

has countably many elements hence cannot equal $\mathbb{R}$. Moreover, $\mathbb{Q} \leq \mathbb{R}$ is a subgroup that by part (b) is not finitely generated.

For (d), denote the group by G. Taking powers of the first generator shows that $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \leq G$ for any $k \in \mathbb{Z}$, and conjugating the first generator by the second shows that $\begin{pmatrix} 1 & 1/2^\ell \\ 0 & 1 \end{pmatrix} \in G$ for any $\ell \in \mathbb{Z}$. Therefore

$$\{k/2^\ell \mid k, \ell \in \mathbb{Z}\} \cong \left\{ \begin{pmatrix} 1 & k/2^\ell \\ 0 & 1 \end{pmatrix} \,\middle|\, k, \ell \in \mathbb{Z} \right\} \leq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \leq G$$

where the first group is viewed as a subgroup of $\mathbb{Q}$ and not finitely generated by part (b) since it is not cyclic. □

Problem 15. Given a set of symbols S and a set of relations R which are words in these symbols, the group $\langle S \mid R \rangle$ is the quotient of the free group generated by S by the normal subgroup generated by R. Find a presentation of the groups $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z}$.

Problem 16. Denote by

$$Q_8 = \left\langle -1, i, j, k \,\middle|\, \begin{array}{c} (-1)^2 = 1 \\ i^2 = j^2 = k^2 = ijk = -1 \\ -1 \text{ is central} \end{array} \right\rangle$$

the *quaternion group*. For $G \in \{Q_8, D_8\}$ do the following:

(a) Show that $|G| = 8$, and write down the multiplication table of G.

(b) Determine the subgroup lattice of G, and optionally for each subgroup determine its normalizer.

(c) Find all 2-element subsets $S \subset G$ such that $\langle S \rangle = G$.

(d) For each $N \trianglelefteq G$, compute the isomorphism class of G/N.

(e) Determine the conjugacy classes of G.

Solution. Here are the answers, without proofs.

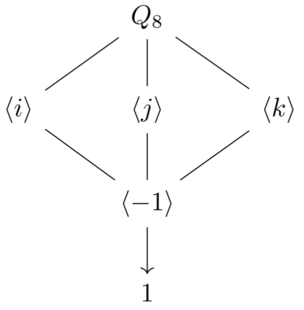
For (a), one can show that

$$G = \{1, -1, i, -i, j, -j, k, -k\}$$

and that the (condensed) multiplication table of G is

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

For (b), the subgroup lattice is as follows:



The normalizer of any subgroup is Q_8, i.e. every subgroup is normal.

For (c), the subsets of order 2 that generate Q_8 are

$$\{\pm i, \pm j\}, \qquad \{\pm i, \pm k\}, \qquad \{\pm j, \pm k\},$$

i.e. 12 subsets.

For (d), the quotient by $\langle -1 \rangle$ is Klein-four.

For (e), the conjugacy classes are $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$. □

Problem 17*. (Do Problem 16 first, or look at the answers to it in Solutions.) Let G be a finite group. Prove or disprove:

(a) If all subgroups of G are normal, then G is abelian.

(b) There exists $H, K \lneq G$, one normal, such that $G = HK$ and $H \cap K = 1$.

(c) There exists an injection $G \hookrightarrow S_{|G|-1}$.

(d) If $H \leq G$, then there exists $N \trianglelefteq G$ such that $G/N \cong H$.

(e) If $N \trianglelefteq G$, then there exists $H \leq G$ such that $G/N \cong H$.

(f) If $H, K \trianglelefteq G$ and $G/H \cong G/K$, then $H \cong K$.

(g) If $H, K \trianglelefteq G$ and $H \cong K$, then $G/H \cong G/K$.

Solution. For (a), all subgroups of Q_8 are normal, but Q_8 is not abelian since $ij = k \neq -k = ji$.

For (b), if $H, K \lneq Q_8$ and $Q_8 = HK$, then H and K must be distinct index 2 subgroups of Q_8, but then $H \cap K = \{-1, +1\}$.

For (c), we will show that in fact Q_8 does not inject into any symmetric group smaller than S_8. Recall that a finite group G acts on a finite set X faithfully if and only if $G \hookrightarrow S_{|X|}$. When $|X| < |G|$, this requires

$$\bigcap_{1 \lneq H \leq G} H = 1,$$

because otherwise if $g \neq 1$ is in this intersection, then

$$[G : G_x] = |Gx| \leq |X| < |G|$$

implies $g \in G_x$ for every $x \in X$. But for Q_8, we have

$$\bigcap_{1 \lneq H \leq Q_8} H = \{-1, +1\}.$$

For (d), there is a copy of $C_4 \cong \langle i \rangle \leq Q_8$, but the only order 4 quotient of Q_8 is $Q_8/\langle -1 \rangle \cong C_2 \times C_2$.

For (e), there is quotient $C_2 \times C_2 \cong Q_8/\langle -1 \rangle$, but the only order 4 subgroups of Q_8 are cyclic.

For (f), observe that

$$\frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}{\langle (1,0), (0,2) \rangle} \cong C_2 \cong \frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}{\langle (0,1) \rangle},$$

but in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we have

$$\langle (1,0), (0,2) \rangle \cong C_2 \times C_2 \ncong C_4 \cong \langle (0,1) \rangle.$$

For (g), observe that in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we have

$$\langle (1,0) \rangle \cong C_2 \cong \langle (0,2) \rangle,$$

but

$$\frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}{\langle (1,0) \rangle} \cong C_4 \ncong C_2 \times C_2 \cong \frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}{\langle (0,2) \rangle}. \qquad \square$$

Remark. Cayley's theorem exhibits an injection $G \hookrightarrow S_{|G|}$ for any finite group G, so part (c) is asking whether this $|G|$ is sharp.

Problem 18*. Show that a transitive group action is the same thing as left-multiplication on a coset space. More precisely, show that if G acts transitively on a set X, then $X \cong G/G_x$ as G-sets for any $x \in X$.

Solution. Let us start with some general facts about maps of G-sets of the form $\varphi\colon G/H \to G/K$:

- for fixed $g \in G$, the function $\varphi(xH) = xgK$ well-defined if and only if
$$hgK = \varphi(hH) = \varphi(H) = gK$$
if and only if $g^{-1}Hg \subset K$
- φ is determined by $\varphi(H)$, since if $\varphi(H) = gK$ for some $g \in G$, then by G-linearity $\varphi(xH) = xgK$ for any $x \in G$
- φ is injective if and only if $xgK = gK$ (i.e. $x \in gKg^{-1}$) implies $x \in H$ if and only if $gKg^{-1} \subset H$
- φ is surjective since for any $y \in G$, we have $\varphi(yg^{-1}H) = yg^{-1}gK = yK$.

Now suppose G acts transitively on a set X. It suffices to show the following two things: $G/G_a \cong G/G_b$ for any $a, b \in X$, and $X \cong G/G_a$ for some $a \in X$.

For the first, since G acts transitively, a and b are in the same orbit, so their stabilizers are conjugate, say $g^{-1}G_a g = G_b$. Then by above, for any $g \in G$, the function $\varphi\colon G/G_a \to G/G_b$ given by $\varphi(xG_a) = xgG_b$ is an isomorphism.

For the second, pick any $a \in X$, and define $f\colon X \to G/G_a$ by $f(b) = gG_a$ where $g \in G$ is such that $ga = b$. This is well-defined because if $ha = b$ for some $h \in G$, then
$$h^{-1}ga = h^{-1}b = a,$$
so $h^{-1}g \in G_a$, i.e. $hG_a = gG_a$. This is surjective since for any $h \in H$, we have $f(ha) = hG_a$. Finally, this is injective because if $f(b) = f(c)$ for some $b, c \in X$, then $ga = b$ and $ha = c$ for $g, h \in G$ where $gG_a = hG_a$, but then
$$b = ga = gg^{-1}ha = gg^{-1}c = c. \qquad \square$$

Problem 19*. Show that a finite group is not the union of the conjugates of one of its proper subgroups.

Solution. Let G be a finite group and $H \leq G$. Since G acts transitively on the conjugates $\mathrm{Conj}_G(H)$ of H, by Problem 18 we have
$$G/N_G(H) = G/G_H \cong \mathrm{Conj}_G(H),$$
so
$$|\mathrm{Conj}_G(H)| = |G/N_G(H)| \leq [G : H].$$

It is now clear that when H is proper G cannot be the union of the conjugates of H because, roughly speaking, the cosets of H partition G whereas the conjugates of H intersect at 1. More precisely

$$\begin{aligned}\left|\bigcup_{K\in\mathrm{Conj}_G(H)} K\right| &\leq |\mathrm{Conj}_G(H)|(|H|-1)+1\\ &\leq [G:H](|H|-1)+1\\ &= |G|-[G:H]+1,\end{aligned}$$

which can equal G only when $G=H$. □

Problem 20*. Let G be a finite group, and let $d\in\mathbb{N}$. Prove and generalize, or disprove:

(*a*) If $d \mid |G|$, then G acts transitively on a set with d elements.

(*b*) If $|G|=144$, then G acts transitively on a set with 9 elements.

Solution. For (a), if G acts transitively on a set X with d elements, then by Problem 18 we have $X\cong G/H$ as G-sets for some $H\leq G$, so G has an index d subgroup. Thus for $G=A_4$ and $d=4$ the statement is false since A_4 does not have a subgroup of order 6 by Problem 10 on Homework 7 (see also remark after Problem 8).

For (b), write $|G|=144=2^4\cdot 3^2$. The first Sylow theorem ensures the existence of a Sylow 2-subgroup P where $|P|=16$, whence G/P is a transitive G-set with 9 elements. □

Problem 21. A group G is *solvable* if there exist subgroups

$$1=N_1\trianglelefteq N_2\trianglelefteq\cdots\trianglelefteq N_{r-1}\trianglelefteq N_r=G$$

such that N_{i+1}/N_i is abelian for $i=1,\dots,r-1$. Prove the following using the isomorphism theorems:

(*a*) A subgroup of a solvable group is solvable.

(*b*) The homomorphic image of a solvable group is solvable.

(*c*) Show that if $N\trianglelefteq G$ and G/N are solvable, then G is solvable.

Problem 22. Show that any p-group or any group G with order pq, p^2q, p^2q^2, or pqr where p,q,r are primes is solvable.

Problem 23. Recall that

$$S_n\cong\left\langle x_1,\dots,x_{n-1}\;\middle|\;\begin{array}{c}x_i^2\text{ for }i=1,\dots,n-1\\(x_ix_{i+1})^3\text{ for }i=1,\dots,n-2\\(x_ix_j)^2\text{ for }i<j\text{ and }|j-i|>1\end{array}\right\rangle$$

via the isomorphism $\tau_i=(i\;i+1)\leftarrow\!\!\!\!\mapsto x_i$.

(a) Two triple transpositions in S_6 share 0, 1, 2, or 3 transpositions. In each case, what is the cycle type of their product?

(b) Find an automorphism $S_6 \to S_6$ that takes transpositions to triple transpositions, and hence is not an inner automorphism.

Problem 24*. Let G be a group. The *commutator* of $x, y \in G$ is defined to be $[x, y] = xyx^{-1}y^{-1}$, and the commutator subgroup $G' \leq G$ is the subgroup generated by all commutators.

(a) Show that G is a abelian if and only if $G' = 1$.

(b) Show that G' is the smallest normal subgroup with abelian quotient, i.e. if $N \trianglelefteq G$ and G/N is abelian, then $G' \leq N$.

(c) Show that any subgroup containing G' is normal.

Solution. For (a), at once G is abelian if and only if $xy = yx$ for all $x, y \in G$ if and only if $[x, y] = 1$ for all $x, y \in G$ if and only if $G' = 1$.

For (b), let $N \trianglelefteq G$ be such that G/N is abelian. Then for all $xN, yN \in G/N$ we have $[x, y]N = [xN, yN] = 1$, i.e. $[x, y] \in N$. Therefore $G' \leq N$.

For (c), let $G' \leq H \leq G$. Then $H/G' \trianglelefteq G/G'$ since G/G' is abelian, so H is normal by the correspondence of normal subgroups under a quotient. □

Problem 25. Show that a proper subgroup of a p-group is properly contained in its normalizer.

Problem 26*. Compute the order of the normalizer $N_{S_p}(C)$ where $C \leq S_p$ is a cyclic subgroup of order p.

Solution. Let $C \leq S_p$ be cyclic of order p. Then $N_{S_p}(C)$ is the stabilizer of C under the conjugation action of S_p in $\mathrm{Conj}_{S_p}(C)$. This action is transitive because the Sylow p-subgroups in S_p are the cyclic order p subgroups, and by the second Sylow theorem these are all conjugate. Moreover, there are $(p-2)!$ subgroups conjugate to C because there are $(p-1)!$ order p elements in S_p and because the subgroups they generate either agree or intersect trivially. Thus by orbit-stabilizer

$$|N_{S_p}(C)| = |S_p|/(p-2)! = p(p-1).$$ □

Problem 27. Let G be a finite group and X a finite G-set. Prove Burnside's lemma:

$$|X/G| = \frac{1}{|G|}\sum_{g \in G} |X^g|.$$

Deduce that a finite group acting transitively on a non-singleton set has a fixed-point-free element.

Problem 28*.

(*a*) (Optional) Prove the following extension of Bézout's identity: For $a, b \in \mathbb{N}$ coprime and $c \geq (a-1)(b-1)$, there exists $x, y \geq 0$ such that $ax+by=c$.

(*b*) Let G be a finite group of order 35. Determine the set of the sizes of the finite G-sets with no fixed points. Optionally, generalize.

Solution. For (*a*), see Answer 70040 on MSE.

For (*b*), let $S(G)$ denote the set (which we wish to compute for $|G| = 35$) of the sizes of the finite G-sets with no fixed points for a finite group G. For any $H \lneq G$, the G-set G/H has no fixed points, so $|G|/|H| \in S(G)$. Moreover, if $a, b \in S(G)$, then $a+b \in S(G)$ by taking a disjoint union, and notice that a G-set has a fixed point if and only if it has an orbit of size 1.

Suppose now $|G| = 35$. There exists a subgroup of order 5 and one of order 7 by Cauchy's theorem, so $35/5 = 7, 35/7 = 5 \in S(G)$. By part (*a*), every number $\geq (5-1)(7-1) = 24$ is in $S(G)$. Conversely, by orbit-stabilizer any orbit must have order dividing 35, so it follows that $S(G)$ is generated (as a monoid) by 5 and 7, i.e. the numbers in $S(G)$ that are less than 24 are

$$5, 7, 10, 12, 14, 15, 17, 19, 20, 21, 22.$$

Therefore

$$S(G) = \{1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\}.$$

The same argument works whenever $|G| = pq$ for p, q distinct primes. □

Problem 29*. Let H be a nontrivial p-group for some prime p.

(*a*) Show that the center of H is nontrivial, using that the size of a conjugacy class in a finite group divides the order of the group.

(*b*) Write $|H| = p^n$ for some $n \geq 1$. Show that H has a subgroup of order p^k for every $0 \leq k \leq n$.

(*c*) Suppose H injects into a finite group G with coprime order. Prove and generalize, or disprove and fix: H contains all elements in G that have order p.

Solution. For (*a*), the cited fact is Problem 2 on Homework 8, whose solution is as follows: a conjugacy class is the orbit of an element under the conjugation action of G on itself, so it divides $|G|$ when G is finite by orbit-stabilizer. Moreover, recall that the conjugacy class of an element has size 1 if and only if the element is central and also that conjugacy classes form a partition. Since $|H| = p^n$ for some $n \geq 1$ and since conjugacy classes of non-central elements have size $\equiv 0 \mod p$, there must be p central elements.

For (*b*), we proceed by induction on n. The $n = 1$ case is trivial, so fix $n > 1$ and suppose every p-group of order p^m for $0 \leq m \leq n$ has subgroups of all possible orders. Suppose $|G| = p^{n+1}$. By part (*a*), the center $Z(G)$ is nontrivial, say $|Z(G)| = p^\ell$ for some $1 \leq \ell \leq n+1$. By the inductive hypothesis the groups $Z(G)$ and $G/Z(G)$ have subgroups of all possible orders, i.e. $Z(G)$

has subgroups of sizes p^k for $0 \leq k \leq \ell$ and $G/Z(G)$ for $0 \leq k \leq n+1-\ell$. The subgroups of $Z(G)$ are already subgroups of G, and the subgroups of $G/Z(G)$ correspond (via the correspondence of subgroups under a quotient) to subgroups of G of sizes p^k for $\ell \leq k \leq n+1$.

For (c), despite H being a Sylow p-subgroup, this is false since H may not be normal in G, i.e. the conjugates of H can contain other order p elements. For example, let $H = C_p$ inject into S_p as the subgroup generated by a p-cycle. By the solution to Problem 26, there are $(p-1)!$ elements of order p in S_p, so certainly H does not contain all elements in S_p of order p when $p \geq 5$.

To fix the statement, add the assumption that H is normal in G. Then if $g \in G$ has order p, it is trivial in G/H because G and H have coprime order, so $g \in H$. □

Problem 30. Suppose G is a finite simple group that has a proper subgroup of index n. Recall that $|G| \mid n!$. Show that in fact $|G| \mid \frac{1}{2}n!$.

Solution. Assume $|G| \geq 3$, since otherwise it is obvious. Consider the injection $G \hookrightarrow S_n$ induced by left-multiplication on cosets of H, where we have used that G is simple. Since A_n is normal in S_n, the preimage $G \cap A_n$ is normal in G, so $G \cap A_n$ is 1 or G. If it is 1, then

$$|GA_n| = |G||A_n| \geq 3|A_n| > |S_n|$$

is absurd. Thus $G \leq A_n$. □

Problem 31. (Optional) The homophonic group H is the group generated by the 26 letters of the English alphabet modulo homophones, i.e. two English words with the same pronunciation are equal in H. Show that H is trivial.

Problem 32. Let G be a group, and let $S, T \leq G$ be subgroups.

(a) Show that $ST = TS$ if and only if $ST \leq G$ if and only if $TS \leq G$.

(b) Show that if S or T is normal, then equivalent statements in part (a) hold.

Solution. For (a), it suffices by symmetry to show that $ST = TS$ if and only if $ST \leq G$.

Suppose $ST = TS$. Recall that a nonempty subset of a group is a subgroup if and only if the subset is closed under differences. Certainly ST is nonempty since $1 \in ST$. Thus, let $st, s't' \in ST$, where $s, s' \in S$ and $t, t' \in T$. Since $t't^{-1}s^{-1} \in TS = ST$, we have $t't^{-1}s^{-1} = s''t''$ for some $s'' \in S$ and $t'' \in T$. Therefore

$$(s't')(st)^{-1} = s't't^{-1}s^{-1} = s's''t'' \in ST,$$

whence $ST \leq G$.

Conversely, suppose $ST \leq G$. If $g \in ST$, then $st = g^{-1} \in ST$ for some $s \in S$ and $t \in T$, so

$$g = (g^{-1})^{-1} = (st)^{-1} = t^{-1}s^{-1} \in TS.$$

On the other hand, if $ts \in TS$ where $t \in T$ and $s \in S$, then

$$ts = ((ts)^{-1})^{-1} = (s^{-1}t^{-1})^{-1} \in ST$$

since $ST \leq G$.

For (b), this is part of the second isomorphism theorem. Spelling it out, if T is normal, then $ST \leq G$ since

$$(s't')(st)^{-1} = s't't^{-1}s^{-1} = s's^{-1}(st't^{-1}s^{-1}) \in ST$$

for any $s, s' \in S$ and $t, t' \in T$, and if S is normal, then a symmetric argument shows that $TS \leq G$. □

Problem 33*. Let G be a group with $N \trianglelefteq G$ and $H \leq G$. Show that the following definitions for G being the inner semidirect product of N and H are equivalent:

(i) $G = NH$ and $N \cap H = 1$

$(i)'$ $G = HN$ and $H \cap N = 1$

(ii) for every $g \in G$, there exists unique $n \in N$ and $h \in H$ such that $g = nh$

$(ii)'$ for every $g \in G$, there exists unique $h \in H$ and $n \in N$ such that $g = hn$

(iii) $H \hookrightarrow G \to G/N$ is an isomorphism

Solution. We will show that

$$(iii) \Leftrightarrow (ii)' \Leftrightarrow (i)' \Leftrightarrow (i) \Leftrightarrow (ii).$$

The equivalence of (i) and $(i)'$ is immediate from Problem 32 since $NH = HN$.

Let us show that (i) and (ii) are equivalent. Suppose (i), and let $g \in G$. For existence, using that $G = NH$, there exists $n \in N$ and $h \in H$ such that $g = nh$. For uniqueness, if $n' \in N$ and $h' \in H$ also satisfy $g = n'h'$, then $n'h' = nh$, so

$$n'n^{-1} = h(h')^{-1} \in N \cap H = 1,$$

i.e. $n' = n$ and $h' = h$. Now suppose (ii). The existence part of the hypothesis ensures $G = NH$. To see that $N \cap H = 1$, let $g \in N \cap H$. Then writing $g = 1g = g1$, the uniqueness part of the hypothesis requires $g = 1$.

By swapping the order of N and H in the above paragraph, we also get that $(i)'$ and $(ii)'$ are equivalent.

Now let us show that $(ii)'$ implies (iii). Supposing $(ii)'$, define the map

$$\begin{aligned} G &\longrightarrow H \\ hn &\longmapsto h, \end{aligned}$$

which is a homomorphism because

$$(hnN)(h'n'N) = hnh'n'N = (hh')((h')^{-1}nh'n') \mapsto hh',$$

where $(h')^{-1}n'h' \in N$ because N is normal. Since N is in the kernel of this map, by the universal property of quotients it factors through G/N. Thus we have the following two maps, where the top map is the one in the hypothesis and the bottom map is the one we have constructed:

$$\begin{tikzcd}
h \arrow[r, mapsto] & hN \\
H \arrow[r, shift left] & G/N \arrow[l, shift left] \\
h & hnN. \arrow[l, mapsto]
\end{tikzcd}$$

These are inverse because

$$h \mapsto hN = h1N \mapsto h \qquad \text{and} \qquad hnN \mapsto h \mapsto hN = hnN.$$

To see that (iii) implies $(ii)'$, suppose (iii). Since $G \to G/N$ has kernel N, the kernel of the composite is $H \cap N$, which is therefore trivial because the composite is an injection. Moreover, the image of the composite is $\{hN \mid h \in H\}$ which is equal to G/N because the composite is a surjection. Thus if $g \in G$, then $gN = hN$ for some $h \in H$, so $h^{-1}g \in N$, i.e. $g = hn$ for some $n \in N$. □

Problem 34*. Show that D_{2n}, where $n \geq 3$, is a nontrivial semidirect product but that neither C_4 nor Q_8 is.

Solution. For D_{2n}, consider the subgroups $\langle s \rangle \leq D_{2n}$ and $\langle r \rangle \trianglelefteq D_{2n}$, which is normal since it is index 2. Then (almost) by definition, any element of D_{2n} can be written uniquely as $s^a r^b$ where $a \in \{0, 1\}$ and $b \in \{0, \ldots, n-1\}$. Therefore D_{2n} satisfies equivalent definition $(ii)'$ in Problem 33.

For $C_4 \cong \mathbb{Z}/4\mathbb{Z}$, the only nontrivial subgroup is $\langle 2 \rangle$, so in order for $\mathbb{Z}/4\mathbb{Z}$ to be a nontrivial semidirect product, we must have

$$N = H = \langle 2 \rangle.$$

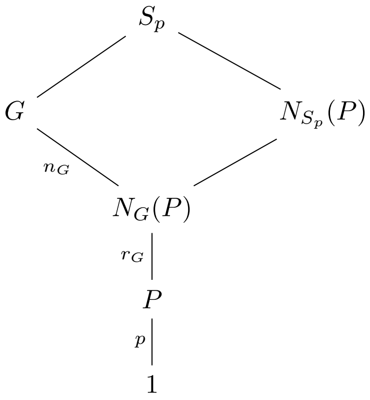
But this violates equivalent definition (i) in Problem 33.

For Q_8, that Q_8 does not satisfy equivalent definition (i) in Problem 33 is exactly the statement of part (b) of Problem 17. □

Problem 35. Let p be a prime, set $X = \{1, \ldots, p\}$, and let $G \leq S_p$ be transitive.

(a) Show that G acts on X transitively if and only if G has a Sylow p-subgroup.

(b) Define n_G and r_G for a Sylow p-subgroup $P \leq G$ as follows:



Show that n_G and r_G are independent of the Sylow p-subgroup $P \leq G$. Note that $|G| = n_G r_G p$ and that $r_G \mid (p-1)$ by Problem 26.

(c) Show that if $r_G = 1$, then $G \cong C_p$.

(d) Suppose $|G| = nrp$ where $r < p$ is also prime, $n > 1$, and $n \equiv 1 \mod p$. Show that $r = r_G$ and $n = n_G$. Moreover, show that any nontrivial $N \trianglelefteq G$ is transitive and that $n_N = n$ and $r_N = r$. Deduce that G is simple.

Solution. For (a), if G acts on X transitively, then $X \cong G/H$ for some $H \leq G$ by Problem 18, so $p = |X| \mid |G|$. Conversely, if $p \mid |G|$, then G contains an element of order p, which must be a p-cycle σ since p is prime, and $\sigma(1), \ldots, \sigma^p(1)$ covers all points of X.

For (b), since Sylow p-subgroups are all conjugate, their normalizers are conjugate, so their normalizers have the same order. This proves the independence. Moreover $N_G(P)$ is the stabilizer of P under the conjugation action of G on the Sylow p-subgroups, so by orbit stabilizer $[G : N_G(P)]$ is size of the orbit of P, i.e. n_p. Finally, $|G| = n_G r_G p$ is just the tower law. Similarly, if $P \leq G$ is a Sylow p-subgroup, then $|N_{S_p}(P)| = p(p-1)$ by Problem 26, so again by the tower law

$$[N_{S_p}(P) : N_G(P)] r_G = [N_{S_p}(P) : P] = p(p-1),$$

where $r_G \nmid p$ implies $r_G \mid (p-1)$.

For (c), our assumption translates to $n_G = |G|/p$. Observe that G contains

$$n_p(p-1) = |G| - n_G$$

elements of order p, none of which have a fixed point. But since $|G_x| = n_G$ for every $x \in X$, by our observation there are exactly n_G elements that fix all of X. Thus $n_G = 1$ since only the identity in S_p fixes all of X.

For (d), note that $r = r_G$ and $n = n_G$, as follows. Since $rn = r_G n_G$, we have $r \equiv r_G \mod p$ by Sylow and by assumption. But $r < p$ by assumption, and

$r_G < p$ since $r_G \mid (p-1)$ by part (b). So $r = r_G$, whence $n = n_G$. Now suppose $1 \lneq N \trianglelefteq G$. The action of N on X is also transitive: its orbits have the same size, namely

$$|N|/|N_x| = |N|/|G_x \cap N|$$

where the $G_x \cap N$ are all conjugate, so since $|X| = p$ and $N \neq 1$, there is only one orbit. Thus

$$|N| = n_N r_N p$$

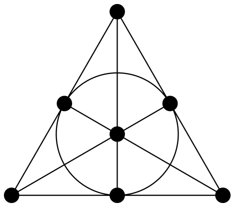
by parts (a) and (b). Moreover, $n_N = n$ since (a) ensures N contains one of the Sylow p-subgroups of G and since normality ensures that N contains the others. Finally, $r_N > 1$ by part (c) because $|N| \geq np > p$ using that $n > 1$, so since

$$nr_N p = |N| \mid |G| = nrp$$

and since r is prime, we have $r_N = r$, i.e. $N = G$. □

Problem 36. A *Steiner system* $S(\ell, m, n)$ for positive integers $\ell < m < n$ is a collection of distinct size-m subsets of $\{1, \ldots, n\}$ called *blocks* such that every size-ℓ subset of $\{1, \ldots, n\}$ is contained in exactly one block. The automorphism group $\mathrm{Aut}(S(\ell, m, n))$ is the subgroup of S_n taking blocks to blocks.

(a) Explain how the following picture depicts a $S(2, 3, 7)$:



(b) Suppose there exists a $S(\ell, m, n)$ for some $\ell \geq 2$. Show that there exists a $S(\ell-1, m-1, n-1)$ such that its automorphism group is a stabilizer subgroup of the action of $S(\ell, m, n)$ on $\{1, \ldots, n\}$. Moreover, show that if $\mathrm{Aut}(S(\ell, m, n))$ is k-transitive, then $\mathrm{Aut}(S(\ell-1, m-1, n-1))$ is $(k-1)$-transitive.

(c) There exists a unique $S(5, 6, 12)$ and a unique $S(5, 8, 24)$. Denote by M_{24} and M_{12} their automorphism groups which are both 5-transitive and which are called *Mathieu groups*. Spam part (b) to fill out or make sense of the first three columns of the following table:

group	order	transitivity	simple	sporadic
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	5		yes
M_{23}				yes
M_{22}				yes
M_{21}			yes	no
M_{20}			no	no
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	5		yes
M_{11}				yes
M_{10}			no	no
M_9			no	no
M_8			no	no

(d) Show that M_{24}, M_{23}, M_{22}, M_{12}, and M_{11} are simple, using that M_{21} is simple (but not sporadic), Problem 35, and the following simplicity criterion, which is Theorem 9.25 in Rotman's *Introduction to the Theory of Groups*. Let X be a faithful k-transitive G-set for some $k \geq 2$, and assume G has a simple stabilizer subgroup. Then the following are true:

- If $k \geq 4$, then G is simple.
- If $k \geq 3$ and $|X|$ is not a power of 2, then $G \cong S_3$ or G is simple.
- If $k \geq 2$ and $|X|$ is not a prime power, then G is simple.

Solution. For (a), label the vertices $1, \ldots, 7$ from top-to-bottom and left-to-right (this is arbitrary), and take the blocks to be the triplets of vertices connected by a line (counting the middle circle), i.e.

$$\{1,2,5\}, \{1,3,7\}, \{1,4,6\}, \{2,3,6\}, \{2,4,7\}, \{3,4,5\}, \{5,6,7\}.$$

It is easy to see that any pair of distinct numbers is in exactly one of these blocks, either by brute force or by observing that any two vertices in the picture uniquely determines a line that they are contained in.

For (b), set $x = n \in \{1, \ldots, n\}$ (by relabeling, we can choose $x \in \{1, \ldots, n\}$), and consider

$$S(\ell-1, m-1, n-1) = \{B - \{x\} \in S(\ell, m, n) \mid x \in B\}.$$

These are indeed blocks of size $\ell - 1$ in $\{1, \ldots, n-1\}$. To see that it is a Steiner system, given a size-$(m-1)$ subset S, there exists a unique block $B \in S(\ell, m, n)$ containing $S \cup \{x\}$, whence $B - \{x\} \in S(\ell-1, m-1, n-1)$ is a unique block containing S. Moreover,

$$\mathrm{Aut}(S(\ell-1, m-1, n-1)) = \mathrm{Aut}(S(\ell, m, n))_x.$$

Finally, the proof of the statement about k-transitivity is similar to the above proof that $S(\ell-1, m-1, n-1)$ is a Steiner system.

For (c), the filled out table, where the fourth column will be determined in part (d), is

group	order	transitivity	simple	sporadic
M_{24}	$3 \cdot 16 \cdot 20 \cdot 21 \cdot 22 \cdot 23 \cdot 24$	5	yes	yes
M_{23}	$3 \cdot 16 \cdot 20 \cdot 21 \cdot 22 \cdot 23$	4	yes	yes
M_{22}	$3 \cdot 16 \cdot 20 \cdot 21 \cdot 22$	3	yes	yes
M_{21}	$3 \cdot 16 \cdot 20 \cdot 21$	2	yes	no
M_{20}	$3 \cdot 16 \cdot 20$	1	no	no
M_{12}	$8 \cdot 9 \cdot 10 \cdot 11 \cdot 12$	sharply 5	yes	yes
M_{11}	$8 \cdot 9 \cdot 10 \cdot 11$	sharply 4	yes	yes
M_{10}	$8 \cdot 9 \cdot 10$	sharply 3	no	no
M_9	$8 \cdot 9$	sharply 2	no	no
M_8	8	sharply 1	no	no

For (d), since 23 and 11 are prime, to show M_{23} and M_{11} are simple it suffices to check the hypotheses in part (d) of Problem 35. Note $M_{23} \leq S_{23}$ acts transitively on $\{1, \ldots, 23\}$ by part (a) of Problem 35 since $23 \mid |M_{23}|$. Since

$$|M_{23}|/23 \equiv 11 \mod 23,$$

it suffices to take

$$r = 11 \quad \text{and} \quad n = |M_{23}|/(11 \cdot 23)$$

because then $|M_{23}| = nrp$ is such that $r < 23 = p$ is prime and $n > 1$ satisfies $n \equiv 1 \mod 23$. Similarly $M_{11} \leq S_{11}$ is transitive since $11 \mid |M_{11}|$, and since

$$|M_{11}|/11 \equiv 5 \mod 11,$$

we may take

$$r = 5 \quad \text{and} \quad n = |M_{11}|/(5 \cdot 11).$$

For M_{24} and M_{12}, note that they have stabilizer subgroups M_{23} and M_{11} respectively by parts (b) and (c). Since M_{23} and M_{11} are simple, by the simplicity criterion M_{24} and M_{12} are automatically simple since they are both 5-transitive. Similarly, M_{22} has stabilizer subgroup M_{21}, which is given in the problem to be simple. Since M_{22} is 3-transitive and since $|M_{22}|$ is clearly not a power of 2, by the simplicity criterion M_{22} is either S_3 or simple, and certainly it is not S_3. □