Homework Problems

(Due Wednesday, December 10, 2025 by 10:00am on WyoCourses)

Instructions: See the syllabus for general expectations regarding homework. In particular, remember that you are encouraged to work together but that anything you submit must be your own work. Work on any subset of these questions that interest you or that you feel comfortable with; you should *not* expect to answer all questions. I suggest that you submit solutions to individual problems as separate documents. (No limit has been set for the number of document submissions in WyoCourses.) Get an early start on your favorite problem, solve it and submit it, then come back to other problems as time permits. Don't wait until December 10. Please check this homework assignment repeatedly online as I intend to add corrections and further hints and comments, as well as a few further problems.

Unless specified otherwise, groups are written multiplicatively.

The *symmetric group* $\mathsf{Sym}\,X$ consists of all permutations of a nonempty set X, i.e. bijections $X \to X$ under composition. A *permutation group on* X is a subgroup $G \leqslant \mathsf{Sym}\,X$. If X is finite, then without loss of generality $X = \{1, 2, \ldots, n\}$ and $G \leqslant S_n$ (a permutation group of degree n).

Elements of X are called *points*; *do not* confuse them with elements of G (which are *permutations* of the points). The image of a point $x \in X$ under a permutation $g \in G$ is sometimes denoted by x^g, or xg, or $g(x)$. The notation $g(x)$ requires 'right-to-left' composition of permutations, so that $(gh)(x) = g(h(x))$. The other notations require 'left-to-right' composition of permutations, so that $x^{gh} = (x^g)^h$ or $x(gh) = (xg)h$. Both conventions are valid; and in fact mathematicians use both choices in different situation. This requires the writer to be clear and consistent in context, identifying their preference to the reader. If you want to use right-to-left composition, you will need to clarify this choice in your solutions.

We say G is *transitive* if for every pair of points $x, x' \in X$, there exists $g \in G$ such that $x' = x^g$. The *stabilizer* of a point $a \in X$ is the subgroup $G_a \leqslant G$ defined by $G_a = \{g \in G : a^g = a\}$. Finally, given two subgroups $H, K \leqslant G$, we naively define their *product* as $HK = \{hk : h \in H,\ k \in K\}$. In general, the product of two subgroups need not be a subgroup (think of the product of two subgroups of order 2 in S_3).

1. **A 'Frattini' argument.** Let $G \leqslant \mathsf{Sym}\, X$ where X is a nonempty set; and let $a \in X$. Show that if G has a transitive subgroup $H \leqslant G$, then $G = G_a H$.

Many books refer to this argument as Frattini's argument exclusively in Sylow theory; yet the same argument pervades all of group theory and I have heard it rightfully referred to as the Frattini argument in the more general context described of #1.

The other thing Frattini was most well known for is his subgroup. If G is a nontrivial group, recall that a *maximal subgroup of* G is a proper subgroup $M < G$ which is not contained in any strictly larger proper subgroup. The Frattini subgroup of G, denoted $\Phi(G) < G$, is by definition the intersection of all maximal subgroups of G. For example, the cyclic group $C_4 = \{1, a, a^2, a^3\}$ has $\Phi(C_4) = \{1, a^2\}$. If G is either of the two groups of order 6, then $\Phi(G) = 1$. If G is either of the two nonabelian groups of order 8, then $\Phi(G) = Z(G)$ has order 2.

2. **Frattini subgroup.** Let G be a nontrivial group, and let $\Phi(G)$ be its Frattini subgroup.
   (a) Prove that $\Phi(G)$ is a proper normal subgroup of G.
   (b) An element $g \in G$ is called a *nongenerator of* G if the following condition is satisfied: Whenever $g, g_1, g_2, \ldots, g_k$ generate G, then the subset $g_1, g_2, \ldots, g_k$ also generates G. (No one bothers to list it in a generating set because it is redundant: no set containing g can be a minimal generating set for G.) Show that $\Phi(G)$ is the set of all nongenerators of G.

The following problem is uniquely unrelated to any of the other problems in this homework set, and unrelated to anything we have talked about in class. It is included here only because it is a personal favourite of mine. It is rather tricky, and I was proud of solving this in my undergraduate algebra class.

3. **Tricky, tricky.** Suppose that G is a finite group with a homomorphism $\phi : G \to G$ (hence an 'endomorphism') such that
   (i) $\phi(\phi(g)) = g$ for all $g \in G$, and
   (ii) $\phi(g) = g$ iff $g = 1$.
   Show that G is abelian.

Bonus points if you can tell me whether the same result holds if G is an infinite group.

A standard result shows that the alternating group A_n of degree n is simple for $n \geqslant 5$. If you are not sure about this or don't quite remember how it is proved, try the following problem. Recall that a nontrivial group G is *simple* iff its only normal subgroups are the trivial subgroup $1 = \{1\}$, and G itself. We write $H \leqslant G$ to say that H is a subgroup of G. Note that a subgroup H is normal in G (written $H \trianglelefteq G$) iff $g^{-1}hg \in H$ for all $h \in H$ and $g \in G$. It is often preferable to restate this condition in the equivalent form $[g, h] \in H$ for all $g \in G$ and $h \in H$, using the commutator $[g, h] = g^{-1}h^{-1}gh$.

4. **Simplicity of the alternating groups.** Let $n \geqslant 5$, and suppose that we have a nontrivial normal subgroup $H \trianglelefteq A_n$; thus $H \neq 1$. Follow these steps to prove that $H = A_n$, thereby concluding that A_n is simple.
   (i) Given a nonidentity element $h \in H$, use commutators $[g, h] \in H$ to obtain a 3-cycle $(i\,j\,k) \in H$. This argument will depend somewhat on the cycle structure of h (the representation of H as a product of disjoint cycles). You may want to start with the case that h has a cycle $(i_1\,i_2\,i_3 \cdots i_k)$ of length $k \geqslant 4$ among its disjoint cycles; then consider what happens if all disjoint cycles in h have length $\leqslant 3$.
   (ii) By showing that any two 3-cycles are conjugate in A_n, show that H contains all three-cycles in A_n.
   (iii) By showing that A_n is generated by its 3-cycles, conclude that $H = A_n$. Thus A_n is simple.

Before trying #5, I recommend doing #4; or at least convincing yourself that you have seen something like #4 before and you are familiar with the arguments. Some level of comfort with infinite sets is also required here. Denote $\mathsf{FinSym}\, X \leqslant \mathsf{Sym}\, X$, the subgroup consisting of all permutations with finite support (where the *support* of $g \in \mathsf{Sym}\, X$ is $\{x \in X : g(x) \neq x\}$).

5. **Infinite symmetric groups.** Let X be an infinite set.
   (a) Show that $\mathsf{FinSym}\, X$ is a nontrivial proper normal subgroup of $\mathsf{Sym}\, X$. Conclude that $\mathsf{Sym}\, X$ is not simple.
   (b) Show that $\mathsf{FinSym}\, X$ has a normal subgroup $\mathsf{Alt}\, X$ of index two. Is $\mathsf{Alt}\, X$ simple?
   (c) Is the quotient group $\mathsf{Sym}\, X / \mathsf{FinSym}\, X$ simple? The answer to this question depends ... on what?

In class (e.g. Sept 3), we used fractional linear transformations as a way to understand $PGL_2(F)$ and $PSL_2(F)$. Here is a slightly different presentation of this same topic which avoids the heuristic of l'Hôpital's Rule.

6. **Fractional linear transformations.** Let $G = GL_2(F)$ where F is an arbitrary field.

   (a) Show that the center of G is the subgroup $Z = \left\{ \left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right] : 0 \neq a \in F \right\}$.

   Denote by P^1F the set of all one-dimensional subspaces of F^2, i.e.

$$P^1F = \{[x] : x \in F\} \cup \{\infty\}$$

   where $[x]$ is the span of $\left[\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right] \in F^2$ and ∞ is the span of $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \in F^2$. This is known as the *projective line over* F. The group $G = GL_2(F)$ permutes the elements of the projective line P^1F; for example the element $\left[\begin{smallmatrix} 2 & 4 \\ 1 & 7 \end{smallmatrix}\right]$ maps $[1] \mapsto \left[\begin{smallmatrix} 3 \\ 4 \end{smallmatrix}\right]$.

   (b) Show that an element $g \in G$ fixes more than two points of the projective line P^1F, iff $g \in Z$.

   The action of G on the projective line gives a homomorphism $G \to \mathsf{Sym}\, P^1F$.

   (c) Show that the kernel of this action is precisely the subgroup Z. (Recall: the *kernel* of a homomorphism is the set of elements mapping to the identity—in this case, the identity permutation.)

   The image of this homomorphism, i.e. the group of all permutations of the projective line induced by G, is the quotient group $PSL_2(F) = G/Z$. This is the *projective special linear group*, whose elements are represented as invertible 2×2 matrices; but where two matrices are identified whenever one is a scalar multiple of the other. Informally, $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ maps $[x] \mapsto \left[\frac{ax+b}{cx+d}\right]$ whenever the denominator is nonzero; and exceptional cases are handled by the heuristic method of 'taking limits'. This action is made precise by our formalism above.

Next we show that the QR-decomposition for square matrices is a consequence of the Frattini argument #1. (Obviously, since we are *proving* existence of the QR-decomposition from first principles, you must not assume it, as that would constitute circular reasoning.)

Let n be a positive integer. Denote by $G = GL_n(\mathbb{R})$ the multiplicative group of invertible $n \times n$ real matrices; and let $O_n(\mathbb{R})$ be the subgroup consisting of orthogonal matrices, i.e. the set of all $A \in GL_n(\mathbb{R})$ such that $AA^T = I$. Here 'T' denotes transpose. Let $\mathcal{X}$ be the set of all 1-dimensional subspaces of $\mathbb{R}^n$; and consider the span of the first standard column vector, $P = \{(a, 0, 0, \ldots, 0)^T : a \in \mathbb{R}\} \in \mathcal{X}$.

7. QR**-decomposition for** G**.** We use the notation introduced above.

   (a) It is pretty clear that G permutes $\mathcal{X}$ transitively. Prove the stronger statement that the subgroup $O_n(\mathbb{R})$ also permutes $\mathcal{X}$ transitively.

   (b) Show that the stabilizer of $P \in \mathcal{X}$ in G, given by $G_P = \{A \in G : AP = P\}$, consists of all invertible matrices whose first column lies in P.

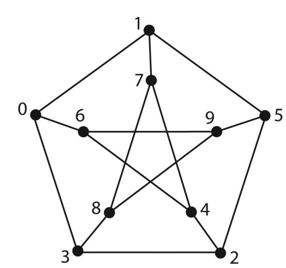
   (c) Use Frattini's argument to show that $G = G_P O_n(\mathbb{R})$.

   (d) Use induction to show that $G = UO_n(\mathbb{R})$ where $U \leqslant G$ is the subgroup consisting of invertible upper-triangular matrices.

   (e) By taking inverses, show that $G = O_n(\mathbb{R})U$.

Note that (e) gives the usual QR-decomposition, as opposed to the 'RQ-decomposition' of (d). Now define a *filtration of* R^n to be a sequence of subspaces $V_1 < V_2 < \cdots < V_n = \mathbb{R}^n$ of dimension $1, 2, 3, \ldots, n$ respectively. (It is not standard to use the term 'filtration' in this way; instead, the Tits theory of buildings calls this a 'maximal flag' or a 'chamber' of the building of type A_{n-1}.) The orthogonal group transitively permutes the set of such filtrations; and the stabilizer of one particular filtration (the 'standard' one) in G, is the subgroup U consisting of all upper triangular matrices. In place of our inductive argument, we could have used instead the action of G on filtrations, to get the QR-decomposition using just one application of the Frattini argument, rather than n or $n{-}1$ separate applications.

The following demonstrates the use of the Frattini argument (similar to #7) for determining the automorphism group of a given graph. I will assume that students trying this problem have some previous experience with graphs and their automorphism groups. Here, we use ordinary graphs (undirected graphs with no loops or multiple edges).



Here we consider the *Petersen graph* P, labelled as shown, so that $G = \operatorname{Aut} P$ is identified as a subgroup of $\mathsf{Sym}\{0, 1, 2, \ldots, 9\} \cong S_{10}$. Many students have seen an argument that P has a group of automorphisms isomorphic to S_5. Some might have also seen that this is the *full* group of automorphisms, so that $G \cong S_5$. It is this result that we aim to prove, without using any prior knowledge of the order or structure of this particular group G.

The stabilizer of a single vertex in G is denoted as usual; thus for example, $G_0 = \{g \in G : g(0) = 0\}$ (using right-to-left composition of permutations). Substitute the condition $0^g = 0$ if you are using left-to-right composition; and clearly indicate which convention you are using. The stabilizer of the pair of vertices $0, 1$ is $G_{0,1} = G_0 \cap G_1$; the pointwise stabilizer of the path $0, 1, 5$ is $G_{0,1,5} = G_{0,1} \cap G_5$, etc. Recall that the size of an orbit $G(x) = \{g(x) : g \in G\}$, for $x \in X$, is given by the orbit-stabilizer formula $|G(x)| = [G : G_x| = |G|/|G_x|$.

8. **Automorphism group G of the Petersen graph P.**
   (a) Let $G_{0,1,5,2}$ be the subgroup consisting of all $g \in G$ fixing the path $0, 1, 5, 2$. Show that $G_{0,1,5,2} = 1$.
   (b) Show that $\alpha = (2\,9)(3\,6)(4\,8)$ generates a subgroup $\langle\alpha\rangle \leqslant G_{0,1,5}$ which acts transitively on $\{2, 9\}$. Deduce that $G_{0,1,5} = G_{0,1,5,2}\langle\alpha\rangle = \langle\alpha\rangle$.
   (c) Next observe that $\beta = (2\,8)(4\,9)(5\,7)$ generates a subgroup $\langle\beta\rangle \leqslant G_{0,1}$ which acts transitively on $\{5, 7\}$. Deduce that $G_{0,1} = G_{0,1,5}\langle\beta\rangle = \langle\alpha\rangle\langle\beta\rangle = \langle\alpha, \beta\rangle$.
   (d) Next observe that $\gamma = (1\,3\,6)(2\,9\,7)(4\,5\,8)$ generates a subgroup $\langle\gamma\rangle \leqslant G_0$ which acts transitively on $\{1, 3, 6\}$. Deduce that $G_0 = G_{0,1}\langle\gamma\rangle = \langle\alpha, \beta\rangle\langle\gamma\rangle = \langle\alpha, \beta, \gamma\rangle$.
   (e) Finally,note that $\delta = (0\,1\,5\,2\,3)(4\,8\,6\,7\,9) \in G$. By merging the orbits of $\alpha, \beta, \gamma, \delta$, observe that $\langle G_0, \delta$ is transitive on the ten vertices and $G = \langle G_0, \delta\rangle G_0 = \langle\alpha, \beta, \gamma, \delta\rangle$.
   (f) Using the orbit-stabilizer formula, deduce that $|G_{0,1,5}| = 2$, $|G_{0,1}| = 4$, $|G_0| = 12$, $|G| = 120$.
   (g) Using any method you know, show that $G \cong S_5$.

Summarizing, G is sharply transitive on the set of 3-arcs of P. Here a 3-arc is a path (i, j, k, ℓ) consisting of three edges (i, j), (j, k), (k, ℓ) which does not repeat any vertex. There are $10 \cdot 3 \cdot 2 \cdot 2 = 120$ such 3-arcs in P; and these are in one-to-one correspondence with the elements of G. So $|G| = 120$.

A similar observation applies to the (2-skeleton of the) 3-cube, a graph H which is 3-regular of order 8 with 12 edges. The graph H has $\operatorname{Aut} H \cong 2 \times S_4$ of order 48, and this group is sharply transitive on 2-arcs. The graph H has $8 \cdot 3 \cdot 2 = 48$ such 2-arcs, so $|\operatorname{Aut} H| = 48$.

Recall that $SL_2(\mathbb{Z})$ is the group of all 2×2 matrices $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ with $a, b, c, d \in \mathbb{Z}$, such that $ad - bc = 1$. Also $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$; see #6.

Take the field $\mathbb{F}_9$ of order 9, and consider fractional linear transformations on the ten-point line $P^1\mathbb{F}_9 = \mathbb{F}_9 \cup \{\infty\}$.

9. **A sporadic isomoprhism.** Show that $PSL_2(9) \cong A_6$. Is $PGL_2(9) \cong S_6$? Explain.

---

10. **Orders of elements in an infinite group.** Let $G = SL_2(\mathbb{Z})$.
    (a) Give explicit examples of elements in G of order 1, 2, 3, 4, 6, and ∞.
    (b) Show that the orders listed in (a) are the only possible orders of elements in G.
    (c) For which values of k does G have a *unique* element of order k? Explain.
    (d) What are the orders of the elements of $PSL_2(\mathbb{Z})$?

    Hint: Consider minimal polynomials. Your life will be much harder if you do not understand minimal and characteristic polynomials of matrices.

In class, we demonstrated using the method of Coxeter-Todd coset enumeration for working with a group presentation $G = \langle X|R\rangle$ to determine $|G|$ and find explicit generators realizing G as a permutation group of small degree. This involves first identifying some large subgroup $H \leqslant G$, and enumerating cosets of H in G. We use an upper bound for $|G| = [G : H]|H|$ using computed values (or upper bounds) for $[G : H]$ and $|H|$; and a lower bound given by the order of a permutation group whose generators we are able to read off explicitly from the table given by the Coxeter-Todd algorithm (since this permutation group is a homomorphic image of G). If the upper and lower bounds agree, then we know the exact value of $|G|$. We are often able to use computational software (as demonstrated in class on October 1, using GAP and Sage) to check our work, and to identify G as a known group up to isomorphism. In #11, follow these steps with the group whose presentation is given. *Work by hand*, then use computational software to check your work.

11. **A group with 2 generators and 3 relations.** Consider the group given by the presentation $G = \big\langle a, b \,:\, a^5 = b^3 = (ab)^2 = 1\big\rangle$.
    (a) Working by hand, use Coxeter-Todd coset enumeration to determine $|G|$. Show your work, including an explanation of your choice of subgroup H.
    (b) Find an explicit permutation representation of small degree for the group G, given by a pair of permutations of small degree satisfying the defining relations. Also identify G as a known group.
    (c) Check your work using appropriate software, such as GAP, Sage, or Magma.

The following problem reverses the process of #11. Here you are first given a group G as a permutation group with explicit generators. From this, you must find an appropriate presentation for G. Work by computer, looking for relations that are satisfied by these generators; and searching for an appropriately small subset of these relations which suffice to define G as a finitely presented group. The best presentation is one which is short and concise, and which yields the correct group G with a modest amount of computational effort. There is no one correct answer, but some answers are much better than others.

12. **Finding a presentation for an explicitly given group.** Consider the permutation group $G = \langle \rho, \sigma \rangle \leqslant S_{14}$ where $\rho = (1,3,5,7,9,11,13)(2,4,6,8,10,12,14)$ and $\sigma = (1,2)(3,6)(4,5)(7,8)(9,12)(10,13)(11,14)$.
   (a) Determine $|G|$.
   (b) Find a presentation of G with two generators and as few relations as possible, and which most readily yields the correct group G.

Recall that the Burnside group $B(m,n)$ is the universal group given by m generators, and with defining relations $g^m = 1$ for every g.

13. **Burnside groups.** Find positive integers m and n such that the Burnside group $B(m,n)$ has *both* of the groups above (in #11 and #12) as homomorphic images. Explain. (You must find m and n such that $B(m,n)$ has normal subgroups K_1 and K_2, such that $B(m,n)/K_1$ and $B(m,n)/K_2$ give the groups in #11 and #12 respectively. Explicit determination of K_1 and K_2, however, is not necessary. Likewise, the explicit determination of $B(m,n)$ is not required; you shouldn't even worry whether this Burnside group is finite or infinite.)

Can you find an easy example of a finitely generated infinite simple group? Some infinite simple groups can be found in #4, but these will probably not be finitely generated. There exist Tarski monsters for large primes p, and these are infinite simple groups which are finitely generated (in fact, 2-generated); but these are only known to exist for extremely large choices of the prime $p > 10^{75}$. The Burnside groups $B(m,n)$ are in general not simple, as pointed out in class. Historically, the first answer to this question is outlined in #16. As a warm-up, you might want to try #14, #15 first.

14. **A group with 2 generators and 2 relations.** Let G be the group generated by two elements a, b subject to the defining relations
$$a^{-1}ba = b^2, \qquad b^{-1}ab = a^2.$$
Show that $G = 1$.

15. **A group with 3 generators and 3 relations.** Let G be the group generated by three elements a, b, c subject to the defining relations
$$a^{-1}ba = b^2, \qquad b^{-1}cb = c^2, \qquad c^{-1}ac = a^2.$$
Show that $G = 1$.

16. **A group with 4 generators and 4 relations.** Let G be the group generated by four elements a, b, c, d subject to the defining relations

$$a^{-1}ba = b^2, \qquad b^{-1}cb = c^2, \qquad c^{-1}dc = d^2, \qquad d^{-1}ad = a^2.$$

(a) Show that the only *finite* group satisfing these relations is the trivial group.

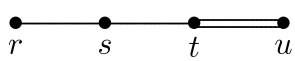
(b) Show that G is nontrivial.

Hints for (a): In any finite group satisfying the given presentation, check that a, b, c, d must be elements of odd order $\geqslant 3$.

Hints for (b): First familiarize yourself with $\langle a, b : a^{-1}ba = b^2 \rangle$, which is an infinite nonabelian group (consider the group generated by $\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$.) Build G from several copies of this group, using free products and amalgamations.

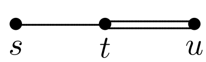
Bonus points: Show that this group G has a homomorphic image G/K which is a finitely generated infinite simple group. Here K is an appropriately chosen normal subgroup of G. As a hint, recall the Frattini subgroup of #2.

Let G be a group with subgroup H. Assuming G is generated by elements $r_1, \ldots, r_k$, recall that the *Schreier graph of* G has vertices given by the right cosets of H in G. For every right coset Hg ($g \in G$) and index i, an edge is drawn from Hg to Hgr_i. (Loops and multiple edges are allowed: If $Hgr_i = Hg$, then we have a loop from this vertex to itself, labelled r_i. If $Hgr_i = Hgr_j$, then an r_i-edge and an r_j-edge are drawn from Hg to the new vertex.) The edges are usually directed edges; but in the case of Coxeter groups, and more generally whenever we have generators of order 2, then undirected edges are used instead. Now consider the Coxeter group $G = W(B_4)$ with Coxeter diagram and presentation as shown:



$$G = \langle r, s, t, u \,|\, r^2, s^2, t^2, u^2, \quad (rs)^3, (st)^3, (tu)^4, (rt)^2, (ru)^2, (su)^2 \rangle$$

Also consider the subgroup $H = W(B_3) < G$, as shown:



$$H = \langle s, t, u \,|\, s^2, t^2, u^2, \quad (st)^3, (tu)^4, (su)^2 \rangle$$

Note that the Schreier diagram has $[G : H]$ vertices. We constructed a few examples in class on September 17–19–22, with the example on September 22 being most pertinent.

17. **Schreier diagram for a Coxeter group.** For the example described above, determine the Schreier graph of G on H. What is the index $[G : H]$?