2022 Fall Honors Algebra Exercise 2 (due on October 6)

For submission, please finish the 20 True/False problems and choose 10 problems from the standard questions and 5 problems from the more difficult ones.

[A] = Artin, [DF] = Dummit and Foote, [DN] = Ding and Nie (Chinese), [H] = Hungerford.

2.1. **True/False questions.** (Only write T or F when submitting the solutions.)

(1) In every cyclic group, every element is a generator.
(2) In a cyclic group of *odd* order, the square of a generator is also a generator.
(3) If an abelian group G is generated by two elements with order p and q (p and q are different primes), then G is cyclic.
(4) Every subgroup of an abelian group is abelian.
(5) In a group G, if x is an element of order p and y is an element of order q, where p and q are distinct prime numbers, then xy has order pq.
(6) If every proper subgroup of a group G is abelian, then G is abelian.
(7) There are same number of even permutations and odd permutations in S_n ($n \geq 2$).
(8) If two normal subgroups H_1 and H_2 of G (as abstract groups) are isomorphic, then $G/H_1 \cong G/H_2$.
(9) Every element of $\mathbf{Z}_4 \times \mathbf{Z}_8$ has order 8.
(10) Every abelian group of order divisible by 6 contains a cyclic subgroup of order 6.
(11) The only homomorphism from A_5 to a group of order 750 is the trivial one.
(12) If H is a normal subgroup of G, then G/H cannot be isomorphic to G.
(13) If the commutator subgroup of a group G is G itself, then G is a simple group.
(14) A group G acts on a set X. If for some $g \in G$, g fixes every element of X, then $g = 1$.
(15) A finite group G acts on a set X. Then for every $x \in X$, $\#G = \#(G \cdot x) \cdot \#\mathrm{Stab}_G(x)$.
(16) A group G acts on a set X. The stabilizer of any two elements $x, y \in X$ are the conjugate of each other.
(17) Let H be a subgroup of G. If the centralizer of H is the entire group G, then H is a subgroup of the center of G.
(18) If a group G contains a cyclic subgroup of order 2 and admits a surjective homomorphism to the cyclic group of order 2, then G can be written as a direct product $G \simeq H \times \mathbf{Z}_2$ for some group H.
(19) Every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ for subgroups $H_1 \leq G_1$ and $H_2 \leq G_2$.
(20) If H is a normal subgroup of G, then for any normal subgroup N of G, HN/H is a normal subgroup of G/H.

2.2. **Warm-up questions.** (Do not turn in the solutions.)

Problem 2.2.1. [DF, page 60, problem 5]
Find the number of generators for $\mathbf{Z}_{49000}$.

Problem 2.2.2. [DF, page 156, problem 2]
Let $G_1, \ldots, G_n$ be groups and let $G := G_1 \times \cdots \times G_n$ be the product. Let I be a proper, nonempty subset of $\{1, \ldots, n\}$ and $J = \{1, \ldots, n\} - I$ its complement. Define G_I to be the set of elements of G that have identity of G_j in position j for all $j \notin I$.

(1) Prove that G_I is isomorphic to the direct product of the groups G_i, $i \in I$.
(2) Prove that G_I is a normal subgroup of G and $G/G_I \cong G_J$.
(3) Prove that $G \cong G_I \times G_J$.

Problem 2.2.3. [DF, page 157, problem 14]
Let $G = A_1 \times \cdots \times A_n$ and for each i let B_i be a normal subgroup of A_i. Prove that $B_1 \times \cdots \times B_n \trianglelefteq G$ and that

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

Problem 2.2.4. Compute the number of non-isomorphic abelian groups of order 576.

Problem 2.2.5. Compute the order of $\mathrm{Aut}(\mathbf{Z}_3 \times \mathbf{Z}_9)$.

Problem 2.2.6. If H is the unique subgroup of G of a given order in G. Show that for any automorphism $\varphi : G \to G$, $\varphi(H) = H$.

Problem 2.2.7. [DF, page 184, problems 1 and 2]
Let H and K be groups and $\varphi : K \to \mathrm{Aut}(H)$ a homomorphism. Write $G = H \rtimes_\varphi K$.

(1) Prove that $C_K(H) = \ker(\varphi)$.
(2) Prove that $C_H(K) = N_H(K)$.

Problem 2.2.8. [DF, page 116, problem 2]
Let G be a group acting faithfully on a set A. Let $\sigma \in G$ and let $a \in A$. Prove that $\sigma \mathrm{Stab}_G(a)\sigma^{-1} = \mathrm{Stab}_G(\sigma(a))$. Deduce that if G acts transitively on A, then

$$\bigcap_{\sigma \in G} \sigma \mathrm{Stab}_G(a)\sigma^{-1} = 1.$$

Problem 2.2.9. [DF, page 116, problem 4]
Let S_3 act on the set Ω of ordered pairs: $\{(i,j) \mid 1 \le i,j \le 3\}$ by $\sigma((i,j)) = (\sigma(i), \sigma(j))$. Find the orbits of S_3 on Ω. For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9 - first fix a labelling of these nine ordered pairs). For each orbit $\mathcal{O}$ of S_3 acting on these nine points pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3.

Problem 2.2.10. Let H and K be subgroups of the group G. For each $x \in G$ define the H-K double coset of x in G to be the set

$$HxK = \{hxk \mid h \in H, k \in K\}.$$

(1) Prove that HxK is the union of the left cosets $x_1K, \ldots, x_nK$ where $\{x_1K, \ldots, x_nK\}$ is the orbit containing xK of H acting by left multiplication on the set of left cosets of K.
(2) Prove that HxK is a union of right cosets of H.

(3) Show that HxK and HyK are either the same set or are disjoint for all $x, y \in G$. Show that the set of $H - K$ double cosets partitions G.
(4) (Alternative to (3)) Consider $H \times K$-action on G given by $(h, k) \cdot g = hgk^{-1}$, where $h \in H, k \in K, g \in G$. Show that this is an action, and the orbit through x is precisely the HxK.
(5) Prove that $\#HxK = \#K \cdot [H : H \cap xKx^{-1}]$.
(6) Prove that $\#HxK = \#H \cdot [K : K \cap x^{-1}Hx]$.

Problem 2.2.11. Find all conjugacy classes and their sizes in the following group:
(1) D_8.
(2) $\mathbf{Z}_2 \times S_3$.
(3) $S_3 \times S_3$.

2.3. **Standard questions.** (Choose 10 problems to submit.)

Problem 2.3.1. Find a product of cyclic groups that is isomorphic to the group

$$(\mathbf{Z}_{12} \times \mathbf{Z}_{12})/\langle(2, 6)\rangle.$$

Problem 2.3.2. Let $\varphi : G \to H$ be a homomorphism of groups. Let K be a subgroup of $\mathrm{Im}(\varphi)$. Show that

$$N_G(\varphi^{-1}(K)) = \varphi^{-1}(N_H(K)).$$

Problem 2.3.3. Let G and H be two groups. Suppose that there is an injective homomorphism $i : H \to G$ and a homomorphism $\pi : G \to H$ such that $\pi \circ i = \mathrm{id}_H$. Show that one can write G as a semidirect product $H \ltimes \ker(\pi)$ such that i is the embedding of H into the first factor, and π is the projection to the first factor (by quotienting out the normal subgroup $\ker(\pi)$).

Can you give an example where this semidirect product is not a direct product?

Problem 2.3.4. [DF, page 166, problem 7]

Let $G = \langle x_1\rangle \times \langle x_2\rangle \times \cdots \times \langle x_n\rangle$ be a finite abelian group (written in multiplicative convention) with $|x_i| = n_i$. Consider the pth power map

$$\varphi : A \to A, \quad \text{by} \quad x \mapsto x^p.$$

(1) Prove that φ is a homomorphism.
(2) Describe the image and the kernel of φ in terms of the given generators. (The answer depends on whether each n_i is divisible by p.)
(3) Prove that both $\ker(\varphi)$ and $A/\mathrm{im}(\varphi)$ are elementary p-groups, namely products of copies of $\mathbb{Z}/p\mathbb{Z}$, and they contain the same number of copies of $\mathbb{Z}/p\mathbb{Z}$.

Problem 2.3.5. [DF, page 167, problem 14]

For any group G define the dual group of G (denoted $\widehat{G}$) to be the set of all homomorphisms from G into the multiplicative group of roots of unity in $\mathbb{C}$ (such homomorphisms are called *characters* of G). Define a group operation in $\widehat{G}$ by pointwise multiplication of functions: if χ, ψ are homomorphisms from G into the group of roots of unity then $\chi\psi$ is the homomorphism given by $(\chi\psi)(g) = \chi(g)\psi(g)$ for all $g \in G$, where the latter multiplication takes place in $\mathbb{C}$.

(1) Show that this operation on G makes $\widehat{G}$ into an abelian group. (In particular, what is the identity element in $\widehat{G}$ and what is the inverse of an element of $\widehat{G}$?)

   Remark on notation: it is better to use $\widehat{G}$ only when G is abelian, as $\widehat{G}$ for G non-abelian often refers to the set of "representations of G.
(2) Show that if G and H are abelian groups, then $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$.
(3) Compute $\widehat{\mathbf{Z}_n}$ as a group.
(4) If G is a finite abelian group, prove that $G \simeq \widehat{G}$.

(This result is often phrased: a finite abelian group is self-dual. It implies that the lattice diagram of a finite abelian group is the same when it is turned upside down. Note however that there is no natural isomorphism between G and its dual (the isomorphism depends on a choice of a set of generators for G). This is frequently stated in the form: a finite abelian group is <u>*non-canonically*</u> isomorphic to its dual.)

Problem 2.3.6. [DF, page 158, problem 17]

Let I be a nonempty index set and let G_i be a group for each $i \in I$. The *restricted direct product* or *direct sum* of the group G_i is the set of elements of the direct product which are identity in all but finitely many components, that is the set of all elements $(a_i)_{i\in I} \in \prod_{i\in I} G_i$ such that $a_i = 1_i$ for all but a finite number of $i \in I$.

(1) Prove that the restricted product is a *normal* subgroup of the direct product.
(2) Let $I = \mathbb{N}$ and let p_i be the ith integer prime. Show that if $G_i = \mathbf{Z}_{p_i}$. Then every element of the restricted direct product of the G_i's has finite order but $\prod_{i\in I} G_i$ has elements of infinite order. Show that in this example, the restricted product is the torsion subgroup of the direct product.

Problem 2.3.7. Let G and H be two groups and let Z be an (abelian) group equipped with embeddings $i : Z \to G$ and $j : Z \to H$ such that the images $i(Z)$ is contained in the center of G, and the image of $j(Z)$ is contained in the center of H.

(1) Show that

$$\begin{aligned} \Delta : Z &\longrightarrow G \times H \\ z &\longmapsto (i(z), j(z)^{-1}) \end{aligned}$$

defines a natural embedding, and the image is a normal subgroup of $G \times H$. Denote $G \times^Z H$ to be the quotient $(G \times H)/\Delta(Z)$.

(2) Consider the following example: $G = \mathrm{GL}_2(\mathbb{R})$, $H = \mathbb{C}^\times := \mathbb{C}\backslash\{0\}$ (with multiplication), and $\mathbb{Z} := \mathbb{R}^\times = \mathbb{R}\backslash\{0\}$. We hope to relate the product $\mathrm{GL}_2(\mathbb{R}) \times^{\mathbb{R}^\times} \mathbb{C}^\times$ to certain unitary group: consider the Hermitian form $\langle -, - \rangle$ with Hermitian matrix $\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ defined on $\mathbb{C}^{\oplus 2}$ and the similitude unitary group:

$$\mathrm{GU}(2) := \big\{ g \in \mathrm{GL}_2(\mathbb{C}),\ c \in \mathbb{R}^\times;\ \langle gx, gy \rangle = c\langle x, y \rangle \big\}.$$

Show that $\mathrm{GL}_2(\mathbb{R}) \times^{\mathbb{R}^\times} \mathbb{C}^\times \cong \mathrm{GU}(2)$.

A version of this isomorphism is used somewhere later in number theory: where the construction for unitary group is easier, yet the construction for GL_2 (or rather its variant) is more subtle. This isomorphism allows one to “transfer” certain structure on $\mathrm{GU}(2)$ to GL_2.

Problem 2.3.8. [DF, page 133–134]

Let H be a normal subgroup of the group G. For each $g \in G$ consider the conjugation on H by $\varphi_g : h \mapsto ghg^{-1}$ for $h \in H$.

Show that sending $G \to \mathrm{Aut}(H)$ by $g \mapsto \varphi_g$ is a homomorphism. The kernel of this map is

$$C_G(H) := \{g \in G;\ gh = hg \text{ for all } h \in H\}.$$

This $C_G(H)$ is called the *centralizer* of H in G.

Problem 2.3.9. [DF, page 177, Proposition 11]

Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:

(1) the identity (set) map between $H \rtimes K$ and $H \times K$ is a group homomorphism (hence an isomorphism),
(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$,
(3) $K \trianglelefteq H \rtimes K$.

Problem 2.3.10. [DF, page 137, problems 3 and 4]

(1) Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images. Deduce that $\#\mathrm{Aut}(D_8) \leq 8$.
(2) Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\mathrm{Aut}(D_8) \cong D_8$. (What is the center of D_{16}?)

Problem 2.3.11. [DF, page 184, problem 6]

Assume that K is a cyclic group, H is an arbitrary group and $\varphi_1, \varphi_2 : K \to \mathrm{Aut}(H)$ be homomorphisms such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite then assume that φ_1 and φ_2 are injective.

Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$. (Challenge question: why the condition of φ_1 and φ_2 being injective when K is infinite is needed?)

Problem 2.3.12. [DF, page 186, problem 18]

Show that for any $n \geq 3$ there are exactly 4 distinct homomorphisms from $\mathbf{Z}_2$ into $\mathrm{Aut}(\mathbf{Z}_{2^n})$. Prove that the resulting semidirect products give 4 nonisomorphic groups of order 2^{n+1}. (Remark: These four groups together with the cyclic group and the generalized quaternion group, $Q_{2^{n+1}}$, are all the groups of order 2^{n+1} which possess a cyclic subgroup of index 2.)

Problem 2.3.13. [DF, page 187, problem 22]

Let F be a field let n be a positive integer and let G be the group of upper triangular matrices in $\mathrm{GL}_n(F)$.

(1) Prove that G is the semidirect product $U \rtimes D$ where U is the set of upper triangular matrices with 1's down the diagonal and D is the set of diagonal matrices in $\mathrm{GL}_n(F)$.
(2) Let $n = 2$. Recall that $U \cong F$ and $D \cong F^\times \times F^\times$. Describe the homomorphism from D to $\mathrm{Aut}(U)$ explicitly in terms of these isomorphisms (i.e., show how each element of $F^\times \times F^\times$ acts as an automorphism on F).

Problem 2.3.14. Let G be a group acting on sets X and Y. We say that a map $f : X \to Y$ is a *G-map* or a *G-equivariant map* if for any $x \in X$,

$$g \cdot f(x) = f(g \cdot x).$$

(1) Show that for $x \in X$, the stabilizer group $\mathrm{Stab}_G(x)$ is a subgroup of $\mathrm{Stab}_G(f(x))$.
(2) Consider the situation $\varphi : X = G/H \to Y = G/K$ for subgroups $H \leq K \leq G$ (sending gH to gK). Show that this map is G-equivariant for the left translation action.

    For a point $y = gK \in Y$, show that its preimage $\varphi^{-1}(y)$ admits a natural transitive action of gKg^{-1}. Write $\varphi^{-1}(y)$ in terms of a coset space of gKg^{-1}.

Problem 2.3.15. Let H be a subgroup of G and let $N := N_G(H)$ denote its normalizer in G. Show that the coset space G/H carries a natural action of $G \times N_G(H)/H$ given by

$$(g, n)xH = gxn^{-1}H$$

for $g \in G$, $n \in N_G(H)$ and $xH \in G/H$.

Show that this action is transitive. What is the stabilizer subgroup at the identity coset H?

Two remarks: having an action of $G \times N_G(H)/H$ is equivalent to say we have an action of G and an action of $N_G(H)/H$, *and the two action commutes*. When we talk about stabilizer subgroup, we really mean a group that *explicitly realized as a subgroup* of $G \times N_G(H)/H$.

Problem 2.3.16. [DF, page 117, problem 9]

Assume that G acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the distinct orbits of H on A.

(1) Prove that G permutes the sets $\mathcal{O}_1, \dots, \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \dots, r\}$ there is a J such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$. Prove that G is transitive on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.

(2) Prove that if $a \in \mathcal{O}_1$ then $\#\mathcal{O}_1 = [H : H \cap \mathrm{Stab}_G(a)]$ and prove that $r = [G : H\mathrm{Stab}_G(a)]$.

The situation considered in this problem will be used quite frequently in studying number theory (in "ramification theory").

Problem 2.3.17. Consider the group S_n acting on $\{1, \dots, n\}$. Let $\mathcal{P}$ denote the set of subsets of $\{1, \dots, n\}$. The natural S_n-action on $\{1, \dots, n\}$ induces an action on $\mathcal{P}$ given by: for $\sigma \in S_n$ and $I \subseteq \{1, \dots, n\}$,

$$\sigma(I) := \{\sigma(i);\ i \in I\}.$$

Find all orbits of $\mathcal{P}$ under this S_n-action. What is the stabilizer of each element of $\mathcal{P}$?

(This generalizes Problem 2.2.9, which may in turn provide some examples to this problem.)

Problem 2.3.18. [DF, page 122, problem 8]

Prove that if H is a subgroup of G of index n, then there is a normal subgroup K of G such that $K \leq H$ and $[G : K] \leq n!$.

Problem 2.3.19. [DF, page 137, problem 8]

Let G be a group with subgroups H and K with $H \leq K$.

(a) Prove that if H is characteristic in K, and K is characteristic in G, then H is characteristic in G.

(b) Give an example to show that if H is normal in K and K is characteristic in G then H need not be normal in G.

Problem 2.3.20. [A, page 229, §1, problem 12]

Let N be a normal subgroup of a group G. Suppose that $\#N = 5$ and that $\#G$ is odd. Prove that N is contained in the center of G.

Problem 2.3.21. [A, page 236, problem 3]

(1) Suppose that a group G operates transitively on a set S, and that H is the stabilizer of an element $s_0 \in S$. Consider the action of G on $S \times S$ defined by $g(s_1, s_2) = (gs_1, gs_2)$. Establish a bijective correspondence between double cosets of H in G and G-orbits in $S \times S$.

(2) Work out the correspondence explicitly for the case that G is the dihedral group D_5 and S is the set of vertices of a 5-gon.

Problem 2.3.22. [DF, page 111, problem 8]

Find a composition series for A_4. Deduce that A_4 is solvable.

Problem 2.3.23. [DF, page 111, problem 12]

Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.

Problem 2.3.24. This problem combines the left translation, the right translation, and the conjugation action of G on itself.

Fix a group G for this discussion.

(1) Show that there is an action of $G \times G$ on G given by: for $(g, h) \in G \times G$, define a bijection:

$$\Phi_{g,h} : G \longrightarrow G$$
$$\Phi_{g,h}(x) = gxh^{-1}.$$

(2) Show that the stabilizer group of this $G \times G$ at each element $g \in G$ is isomorphic to G. (Note: these subgroups are isomorphic but *not* the same as a subgroups.)

(3) Show that the left translation, right translation, and the adjoint actions maybe viewed as restrictions of this $G \times G$-action to certain subgroups of $G \times G$.

2.4. **More difficult questions.** (Choose 5 problems to submit)

Problem 2.4.1. Let p be a prime. Write the following abelian groups additively.

(1) Consider the group $G = \mathbf{Z}_{p^{m_1}} \times \cdots \times \mathbf{Z}_{p^{m_r}}$ with $m_1 \leq \cdots \leq m_r$. Compute the order of p^n-torsion subgroup of G:

$$G[p^N] := \{x \in G;\ p^N x = 0\}$$

(2) Let $H = \mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_s}}$ be another abelian group with $n_1 \leq \cdots \leq n_s$. Show that $G \simeq H$ if and only if $r = s$ and $m_i = n_i$ for each $i = 1, \dots, r$.

Problem 2.4.2. [Yau contest, 2019]

Let S_n be the group of permutations of $\{1, \dots, n\}$. Let $\sigma \in S_n$ be the permutation

$$(1, n)(2, n-1) \cdots (k, n-k+1) \cdots \left(\left\lceil \tfrac{n-1}{2} \right\rceil, \left\lceil \tfrac{n+2}{2} \right\rceil\right).$$

Prove that the centralizer $Z_{S_n}(\sigma)$ is isomorphic to $S_{\lfloor \frac{n}{2} \rfloor} \ltimes (\mathbf{Z}_2)^{\lfloor n/2 \rfloor}$.

Problem 2.4.3. Let G be a group of order n with n odd. Prove that the left translation action gives a homomorphism $G \to A_n$.

Problem 2.4.4. Let G be a finitely generated abelian group. The classification theorem says that G is isomorphic to product to "standard" abelian groups. But such isomorphism is not "canonical". We discuss this matter here. We write the group operation in G additively. Let us assume that $G \simeq \mathbb{Z} \times \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_r}$ for positive integers $n_1 \geq 2$, $n_i | n_{i+1}$ for $i = 1, \dots, r-1$.

(1) Define $G_{\mathrm{tor}} := \{g \in G;\ n \cdot g = 0 \text{ for some } n \in \mathbb{N}\}$; this is the torsion subgroup of G. Show that if G is isomorphic to $\mathbb{Z} \times \mathbf{Z}_{n_1} \times \cdots \times \mathbf{Z}_{n_r}$ and $G/G_{\mathrm{tor}} \cong \mathbb{Z}$. (This G_{tor} is a canonical subgroup and $G/G_{\mathrm{tor}} \cong \mathbb{Z}$ is a canonical torsion-free quotient.)

(2) Describe all injective homomorphisms $\varphi : \mathbb{Z} \to G$ such that $G/\varphi(\mathbb{Z})$ is isomorphic to G_{tor}. How many are there?

Show that every such φ induces an isomorphism $\tilde{\varphi} : \mathbb{Z} \times G_{\mathrm{tor}} \to G$. (But of course, there is no canonical such choice.)

Problem 2.4.5 (Yau contest 2017)**.** Let A be a finite abelian group and let $\phi : A \to A$ be an endomorphism. Put

$$A_{\mathrm{nil}} := \left\{x \in A \;\middle|\; \phi^k(x) = 0 \text{ for some } k \geq 1\right\}.$$

Show that there is a unique subgroup A_0 of A such that ϕ restricts to an automorphism of A_0 and $A = A_0 \times A_{\mathrm{nil}}$.

This problem seems a little strange if one sees it the first time. A good example is the following: let p be an odd prime and $r \in \mathbb{N}$, $A = \mathbf{Z}_{p^r}^4$; the homomorphism ϕ is given by the matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & p \end{pmatrix}$$

The decomposition $A = A_0 \times A_{\mathrm{nil}}$ is used for example in p-adic number theory.

Problem 2.4.6. [Proposed by Yuan]

Let G be an finite $\mathbb{Z}$-module (i.e., a finite abelian group with additive group law) with a bilinear, (strongly) alternative, and non-degenerate pairing

$$\ell : G \times G \to \mathbb{Q}/\mathbb{Z}.$$

Here "(strongly) alternating" means for every $a \in G$, $\ell(a,a) = 0$; "non-degenerate" means for every nonzero $a \in G$ there is a $b \in G$ such that $\ell(a,b) \neq 0$. Show in steps the following statement:

(S) : G is isomorphic to $H_1 \oplus H_2$ for some finite abelian groups $H_1 \simeq H_2$ such that

$$\ell_{H_i \times H_i} = 0 \quad \text{for each } i = 1, 2.$$

(1) For every $a \in G$, write $o(a)$ for the order of a and $\ell_a : G \to \mathbb{Q}/\mathbb{Z}$ for the homomorphism $\ell_a(b) = \ell(a,b)$. Show that the image of ℓ_a is $o(a)^{-1}\mathbb{Z}/\mathbb{Z}$.

(2) Show that G has a pair of elements a, b with the following properties:
  (a) $o(a)$ is maximal in the sense that for any $x \in G$, $o(x)|o(a)$;
  (b) $\ell(a,b) = o(a)^{-1} \bmod \mathbb{Z}$;
  (c) $o(a) = o(b)$.

  We call the subgroup $\langle a, b\rangle := \mathbb{Z}a + \mathbb{Z}b$ a *maximal hyperbolic subgroup* of G.

(3) Let $\langle a, b\rangle$ be a maximal hyperbolic subgroup of G. Let G' be the orthogonal complement of $\langle a, b\rangle$ consisting of elements $x \in G$ such that $\ell(x, c) = 0$ for all $c \in \langle a, b\rangle$. Show that G is a direct sum as follows:

$$G = \mathbb{Z}a + \mathbb{Z}b + G'.$$

(4) Finish the proof of (S) by induction.

One origin of such group G is the so-called Tate–Shafarevich group of an elliptic curve over a number field. Such group comes equipped with a perfect alternating pairing IF known to be finite.

Problem 2.4.7. [DF, page 138, problem 18]

This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.

(1) Prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e., for each $\sigma \in \mathrm{Aut}(G)$ and each conjugacy class C of G the set $\sigma(C)$ is also a conjugacy class of G.

(2) Let C be the conjugacy class of transpositions in S_n and let C' be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|C| \neq |C'|$. (Here we use $n \neq 6$.) Deduce that any automorphism of S_n sends transpositions to transpositions.

(3) Prove that for each $\sigma \in \mathrm{Aut}(S_n)$

$$\sigma : (12) \mapsto (ab_2), \quad \sigma : (13) \mapsto (ab_3), \quad \ldots, \quad \sigma : (1n) \mapsto (ab_n)$$

  for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, \ldots, n\}$.

(4) As we have known that $(12), (13), \ldots, (1n)$ generate S_n, deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (3) to show that S_n has at most $n!$ automorphisms and conclude that $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ for $n \neq 6$.

(Comment: before teaching this class, I had no idea of this! So strange. If you are interested, read on for [DF, page 138, problem 19] and [DF, page 221, problem 10].)

Problem 2.4.8. [DN, page 100, problem 57]

Prove that if a group G is finitely generated, then any its subgroup of finite index is finitely generated.

Problem 2.4.9 (wreath product). [DF, page 187, problem 23] + some content online

Let K and L be groups, let n be a positive integer, let $\rho : K \to S_n$ be a homomorphism and let H be the direct product of n copies of L. Then there is a natural homomorphism $\psi : S_n \to \mathrm{Aut}(H)$, by permuting the n factors of H. The composition $\psi \circ \rho$ is a homomorphism from K into $\mathrm{Aut}(H)$. The wreath product of L by K is the semidirect product $H \rtimes K$ with respect to this homomorphism and is denoted by $L \wr K$ (LaTeX code \wr) (this wreath product depends on the choice of permutation representation ρ of K and of course the number n - if none is given explicitly, ρ is assumed to be the left regular representation of K).

(1) Assume K and L are finite groups and ρ is the left regular representation of K. Find $\#(L \wr K)$ in terms of $\#K$ and $\#L$.
(2) Let p be a prime, let $K = L = Z_p = \mathbb{Z}/p\mathbb{Z}$ and let ρ be the left regular representation of K. Prove that $Z_p \wr Z_p$ is a non-abelian group of order p^{p+1} and is isomorphic to a Sylow p-subgroup of S_{p^2} (the permutation group of p^2 elements).
(3) Show that $S_2 \wr S_n$ (Hyperoctahedral group) is the symmetry group of n-dimensional cube. The action of S_n on $\{1, \ldots, n\}$ is the usual one.

Some fun examples:

(a) The Rubik's Cube group is a subgroup of index 12 in the product of wreath products, $(Z_3 \wr S_8) \times (Z_2 \wr S_{12})$, the factors corresponding to the symmetries of the 8 corners and 12 edges.
(b) The Sudoku validity preserving transformations (VPT) group contains the double wreath product $(S_3 \wr S_3) \wr S_2$, where the factors are the permutation of rows/columns within a 3-row or 3-column band or stack (S_3), the permutation of the bands/stacks themselves (S_3) and the transposition, which interchanges the bands and stacks (S_2). Here, the index sets Ω are the set of bands (resp. stacks) ($|\Omega| = 3$) and the set bands, stacks ($|\Omega| = 2$). Accordingly, $\#\big((S_3 \wr S_3) \wr S_2\big) = (3!)^8 \times 2$.

Problem 2.4.10. [DF, page 122, problem 14]

Let G be a finite group of composite order n with the property that G has a subgroup of order k for each positive integer k dividing n. Prove that G is not simple.

Problem 2.4.11. [DF, page 131, problems 23–24]

(1) Recall that a proper subgroup M of G is called *maximal* if whenever $M \leq H \leq G$, either $H = M$ or $H = G$. Prove that if M is a maximal subgroup of G then either $N_G(M) = M$ or $N_G(M) = G$. Deduce that if M is a maximal subgroup of G that is not normal in G then the number of nonidentity elements of G that are contained in conjugates of M is at most $(\#M - 1)[G : M]$.

(2) Assume H is a proper subgroup of the finite group G. Prove

$$G \neq \bigcup_{g \in G} gHg^{-1},$$

i.e., G is not the union of the conjugates of any proper subgroup.

Remark: This problem has the following application later in number theory: Let L be a finite extension of a number field K. Then there exists infinitely many unramified places v of K such that every place of L over v has degree > 1 over v.

Problem 2.4.12. (Cohen–Lenstra density question)

(1) Let p be a prime. Compute the order of automorphism group of

$$\mathbf{Z}_{p^{n_1}} \times \cdots \times \mathbf{Z}_{p^{n_r}}$$

with $n_1 \leq \cdots \leq n_r$.

(2) Define $(p)_r := \prod_{i=1}^{r}(1 - p^{-i})$. Show that

$$\sum_{\substack{G\ p\text{-abelian} \\ \#G \leq p^r}} \frac{1}{\#\mathrm{Aut}(G)} = \frac{1}{(p)_r},$$

where the sum takes over all finite abelian groups that have order $\#G | p^r$. (I have not tried this problem myself but I have checked it for $r = 2, 3$ by hand; I don't know if there is a nice proof.)

Taking the limit shows that

$$\sum_{G\ p\text{-abelian}} \frac{1}{\#\mathrm{Aut}(G)} = \frac{1}{(p)_\infty},$$

Remark: The background of this question is the so-called Cohen–Lenstra heuristic. Consider all imaginary quadratic fields $F = \mathbb{Q}(\sqrt{-d})$ with d a square-free positive integer. Its "ring of integers"

$$\mathcal{O}_F = \begin{cases} \mathbb{Z}[\sqrt{-d}] & -d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-d})] & -d \equiv 1 \bmod 4. \end{cases}$$

Then there is a question of whether $\mathcal{O}_F$ has a property that every element admits a unique factorization into primes, just like in $\mathbb{Z}$. This is of course not correct in general. To characterize the failure of this, one may naturally introduce a finite abelian group, called the *ideal class group* $\mathrm{Cl}(\mathcal{O}_F)$. The group $\mathrm{Cl}(\mathcal{O}_F)$ is trivial if and only if $\mathcal{O}_F$ admits the unique factorization property. For imaginary quadratic fields F, it is known (Gauss' conjecture) that there are only 9 imaginary quadratic fields. Cohen–Lenstra says that for any finite abelian group G of p-power order

$$\lim_{D \to \infty} \frac{\#\{1 < d \leq D \text{ square-free} \mid \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}(\sqrt{-d})})[p^\infty] \cong G\}}{\#\{1 < d \leq D \text{ square-free}\}}$$

is proportional to $\dfrac{1}{\#\mathrm{Aut}(G)}$. (Here $\bullet[p^\infty]$ means to take the p-power torsion subgroup of the corresponding abelian group, or the p-Sylow subgroup.) This is the "correct" randomness: namely, the ideal class group is a "random" finite abelian group, weighted by the size of its automorphism group.

For real quadratic fields, there is also a similar conjecture, but more complicated heuristic (namely the ideal class group is supposed to be a random group quotient by a random cyclic subgroup). In particular, conjecturally, around 75.446% of real quadratic fields have the unique factorization property; it is not even known to have infinitely many such real quadratic field (known as Gauss' conjecture on real quadratic fields).

Problem 2.4.13 (Alibaba 2022)**.** Let $G_1, \ldots, G_n$ be nonabelian simple groups for some integer $n \geq 2$; and let H be a group of $G_1 \times \cdots \times G_n$ satisfying that the projection homomorphism $H \to G_i \times G_j$ is surjective for every pair of indices $i < j$. Show that $H = G_1 \times \cdots \times G_n$.