Math 561/661 **Fall 2018**
Homework 6 **Drew Armstrong**

---

1. The Alternating Group A_4 is Not Simple. Recall that $A_4 \subseteq S_4$ is the subgroup of permutations of $\{1,2,3,4\}$ which can be expressed as the product of an even number of transpositions.

(a) Prove that the following set is a normal subgroup:

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4.$$

It follows that A_4 is not a simple group.

(b) Furthermore, prove that $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The letter V is for *Klein's Viergruppe*. [Once upon a time it was surprising that not every abelian group is cyclic.]

2. Primary Factors of a Finite Abelian Group. Let G be finite abelian group.

(a) Suppose that there exist subgroups $H, K \subseteq G$ such that $\#G = \#H \cdot \#K$ and $\gcd(\#H, \#K) = 1$. In this case, prove that G is an internal direct product:

$$G = H \times K.$$

(b) Now suppose that $\#G = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$. The Sylow Theorems tell us that for each i there exists a unique subgroup $H_i \subseteq G$ of size $\#H = p_i^{e_i}$. Use part (a) and induction to prove that G is the direct product of these subgroups:

$$G = H_1 \times H_2 \times \cdots \times H_k.$$

This is called the *primary factorization* of G. It also true that each *primary factor* H_i is a product of cyclic subgroups but this is harder to prove.

(c) In the special case that G is **cyclic**, prove that

$$G \cong \frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_2^{e_2}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{e_k}\mathbb{Z}}.$$

This is a non-constructive version of the Chinese Remainder Theorem.

3. Lagrange vs. Rank-Nullity. Let $p \in \mathbb{Z}$ be prime. You showed on the previous homework that every nonzero element of the ring $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse. In other words, $\mathbb{F}_p$ is a field of size p.

(a) Let V be an n-dimensional vector space over $\mathbb{F}_p$. Prove that $\#V = p^n$.

(b) Now let $U \subseteq V$ be a k-dimensional subspace. Show that Lagrange's Theorem and the Rank-Nullity Theorem give you the same information about this subspace.

4. Double Cosets. Let G be a group and let $H, K \subseteq G$ be any subgroups. For each pair $(h,k) \in H \times K$ consider the function $\varphi_{h,k}(g) := hgk^{-1}$.

(a) Prove that this defines a group homomorphism $\varphi : H \times K \to \mathrm{Perm}(G)$.

(b) For each $g \in G$, prove that the orbit satisfies

$$\mathrm{Orb}_\varphi(g) = HgK := \{hgk : h \in H, k \in K\}.$$

These orbits are called *double cosets*. Unlike single cosets, we will see that double cosets do not all have the same size.

(c) We also have a group action $\psi : H \to \mathrm{Perm}(G/K)$ defined by $\psi_h(gK) := (hg)K$. (Don't bother to prove this.) For all $g \in G$ prove that HgK is the disjoint union of the cosets in the ψ-orbit of gK:

$$HgK = \coprod_{C \in \mathrm{Orb}_\psi(gK)} C.$$

(d) For all $g \in G$ prove that $\mathrm{Stab}_\psi(gK) = H \cap gKg^{-1}$, where $gKg^{-1} := \{gkg^{-1} : k \in K\}$.

(e) Combine (c) and (d) with Lagrange's Theorem and Orbit-Stabilizer to conclude that

$$\#HgK = \frac{\#H \cdot \#K}{\#(H \cap gKg^{-1})}.$$

5. Burnside's Lemma. Let $\varphi : G \to \mathrm{Perm}(X)$ be a group action, and let X/G denote the set of orbits. For each $g \in G$, let $\mathrm{Fix}_\varphi(g)$ denote the set of elements fixed by g:

$$\mathrm{Fix}_\varphi(g) := \{x \in X : \varphi_g(x) = x\} \subseteq X.$$

(a) Count the elements of the set $\{(g, x) \in G \times X : \varphi_g(x) = x\}$ in two ways to prove that

$$\sum_{g \in G} \#\mathrm{Fix}_\varphi(g) = \sum_{x \in X} \#\,\mathrm{Stab}_\varphi(x).$$

(b) Use Orbit-Stabilizer to obtain a formula for the number of orbits:

$$\#(X/G) = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}_\varphi(g).$$

(c) Application: Consider a "bracelet" (circular string of beads) containing 6 beads. There are k possible colors for the beads, and we regard two bracelets to be the same if they are equivalent up to dihedral symmetry. Use the formula in part (b) to compute the number of different bracelets. [Hint: The dihedral group D_{12} acts on a set X of size k^6. You want to compute the number of orbits: $\#(X/D_{12})$. To get started I'll tell you that $\#\mathrm{Fix}(R) = k$ and $\#\mathrm{Fix}(R^2) = k^2$.]

Problems 6 and 7 are only for Sanjoy Kundu.

6. Normal Subgroups of S_n. Assuming that A_n is simple (which is true for $n \geq 5$) you will prove that A_n is the only non-trivial normal subgroup of S_n.

(a) Prove that the center of S_n is trivial: $Z(S_n) = \{\mathrm{id}\}$. [Hint: Recall that a group element $g \in G$ is in the center if and only if its conjugacy class has size 1.]

(b) Suppose that $N \trianglelefteq S_n$ is a normal subgroup not equal to $\{\mathrm{id}\}$ or S_n. Use the fact that A_n is simple to prove that $N = A_n$ or $\#N = 2$. [Hint: Consider $N \cap A_n \trianglelefteq A_n$.]

(c) Continuing from (b), if $\#N = 2$ then we must have $N = \{\mathrm{id}, \tau\}$ for some $\tau \in S_n$ such that $\tau \neq \mathrm{id}$ and $\tau^2 = \mathrm{id}$. Prove that $\tau \in Z(S_n)$ and get a contradiction.

7. Gaussian Binomial Coefficients. Let p be prime and consider the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(a) For all $n \geq 0$ we define the *p-factorial*:

$$[n]_p! := \prod_{i=0}^{n-1} (1 + p + p^2 + \cdots + p^i) \in \mathbb{Z}.$$

Prove that $\#GL_n(\mathbb{F}_p) = p^{\binom{n}{2}} \cdot (p-1)^n \cdot [n]_p!$. [Hint: The columns of an invertible matrix are just an ordered basis for the vector space $\mathbb{F}_p^n$. Argue that there are $p^n - 1$ ways to choose the first basis vector, then $p^n - p$ ways to choose the second basis vector, etc., so that $\#GL_n(\mathbb{F}_p) = \prod_{i=0}^{n-1}(p^n - p^i)$.]

(b) Let X be the set of all k-dimensional subspaces of $\mathbb{F}_p^n$. The group $GL_n(\mathbb{F}_p)$ acts on X in the obvious way. For any k-dimensional subspace $U \in X$, prove that the stabilizer of U is isomorphic to the following subgroup of $GL_n(\mathbb{F}_p)$:

$$\left\{ \left(\begin{array}{c|c} A & C \\ \hline 0 & B \end{array} \right) : A \in GL_k(\mathbb{F}_p), B \in GL_{n-k}(\mathbb{F}_p), C \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{F}_p) \right\}.$$

[Hint: Choose a basis $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_n$ for $\mathbb{F}_p^n$ such that $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ is a basis for U.]

(c) Combine parts (a) and (b) with the Orbit-Stabilizer Theorem to prove that

$$\#X = \frac{[n]_p!}{[k]_p! \cdot [n-k]_p!}.$$

This is called a *Gaussian binomial coefficient*.