Abstract Algebra for Putnam

November 4, 2026

Definitions

Definition 1. *A **group** G is a set with an operation $a * b$ so that*

- *(Identity) There exists an element $1 \in G$ so that $1 * g = g * 1 = g$*
- *(Associativity) $(a * b) * c = a * (b * c)$*
- *(Inverse) For all $a \in G$ there exists $a^{-1} \in G$ with $a * a^{-1} = a^{-1} * a = 1$.*

*We say a group is **abelian** if $a * b = b * a$.*

An **endomorphism** in general means a "function" from something to itself; groups usually show up as **automorphisms**, which are those endomorphisms that have an inverse. If for some reason in your life you find yourself looking at endomorphisms, then you should simply drop the inverse assumption from the definition of a group and what you will be working with is called a **monoid**, but we won't talk about those.

Definition 2. *We say a group G is **finitely generated** if there exists a finite set $g_1, ..., g_n \in G$ so that any element is written as a finite product of these.*

Theorem 1 (Smith Normal Form)**.** *Let A be a finitely generated abelian group. Then*

$$A \cong \bigoplus_{i=1}^{r} \mathbb{Z} \bigoplus_{p \text{ is prime}} \mathbb{Z}/p^{e_p}$$

with only finitely many primes.

Definition 3. *A **ring** R is a set endowed with a notion of addition and multiplication. It has an operation $+$ under which it is an abelian group (with identity element 0) and it has a multiplication $*$ under which it is a monoid (group with no inverse) and it satisfies distributivity meaning*

- $a * (b + c) = (a * b) + (b * c)$
- $(b + c) * a = (b * a) + (c * a)$.

*We say it is **commutative** if $a * b = b * a$.*

Problem List

The following are meant to convince you that groups are really automorphisms.

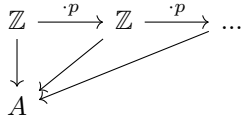
Problem 1. *Show that the following are groups:*

- *Invertible matrices of size $(n \times n)$ with with values in any ring (part of this is to check that a matrix with values in a ring makes sense).*
- *Real-valued matrices of size $(n \times n)$ that preserve the dot product*
- *For $n \geq 3$, consider the points $\left(cos(2\pi \frac{i}{n}),\ sin(2\pi \frac{i}{n})\right)$ for $0 \leq i < n$. Show that (2×2) matrices that preserve this set (i.e. any one of these points maps to another one of these points) is a group.*
- *For all the above, show that those with determinant 1 give a subgroup.*
- *Bijections of a set*

Problem 2. *Say X is a set and let $\mathbb{Z}[X]$ be the set of finite formal sums of elements of X i.e. an element can be written as a finite sum $\sum_{i=1}^{n} n_i s_i$ for $n_i \in \mathbb{Z}$ and $s_i \in X$.*

- *Show that this is an abelian group.*
- *Say X is a group, show that this makes $\mathbb{Z}[X]$ a ring.*
- *Show that a homomorphism of abelian groups groups $\mathbb{Z}[X] \to A$ are in bijection with functions of sets $X \to A$.*

Problem 3. *Consider a commutative diagram of the form*



for some group A. Show that the data of the commuting maps into A is the same as a homomorphism into A out of $\mathbb{Z}[1/p]$; this is the subgroup of the rationals where the denominator is only allowed to be a power of p.

Definition 4. *Let $g \in G$ and a subgroup $H \leq G$. We define gH to be the set of elements of the form gh for $h \in H$ as the **right coset** of H. The left cosets are similarly defined.*

Definition 5. *The **order** of a finite group group $|G|$ is the number of elements. The order of an element $\mathrm{ord}(g)$ is the smallest $n \geq 1$ so that $g^n = 1$.*

Problem 4. *Let G be a finite group.*

- *For $H \leq G$, show $|H|$ divides $|G|$. We call $[G : H] := |G|/|H|$ the **index** of H in G.*

- *Show that the index makes sense for the subgroup $n\mathbb{Z} \subset \mathbb{Z}$ although these aren't finite groups; what is the index in this case?*

Definition 6. *We say a subgroup $N \leq G$ is **normal** if for all $n \in N$ and $g \in G$, $g^{-1}ng \in N$.*

Problem 5. *Show the following things:*

- *Come up with an example or a normal subgroup and a non-normal subgroup.*
- *Show that $N \leq G$ is normal if and only if $gN = gN$ for all $g \in G$ i.e. left and right cosets agree.*
- *Show that an index 2 subgroup is normal.*
- *Show that in an abelian group, all subgroups are normal.*
- *Show that the intersection of normal subgroups is normal.*
- *Show that the kernel of a homomorphism is normal. If the homomorphism is surjective, show that this is the same as quotienting out by the kernel.*

Theorem 2. *Say $N \leq G$ is a normal subgroup. Then the quotient G/N (formed by $g \sim g'$ if $g' = ng$ for some $n \in N$) is a group called the **quotient group**.*

Problem 6. *Show the previous theorem; here are two key things to prove:*

- *Show that the above gives an equivalence relation so G/N is well-defined.*
- *Show that the group structure is well-defined (this crucially uses normality!).*

Problem 7. *Show that $x \mapsto e^{ix}$ gives a homomorphism from the real numbers to the unit complex numbers, which can be identified with a circle. Show that the kernel is $2\pi\mathbb{Z}$ and thus $S^1 \cong \mathbb{R}/2\pi\mathbb{Z}$. Is this finitely generated?*

Problem 8. *Show that any finite group can be obtained as a subgroup of Σ_n, the group of bijections of a set with n elements.*

Problem 9. *Classify which of the above are*

- *abelian*
- *finitely generated*
- *if there are subgroups, are they normal?*

Problem 10. *Show that the following are rings: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, $R[t]$ polynomials in t with coefficients in R, $R[t^{\pm 1}]$ Laurent polynomials in t with coefficients, $R[[t]]$ power series in t with coefficients in R.*

The ones from here on are harder.

Problem 11. *Consider a 6-sided die. You could move this around in space and put it back so it looks the same: for example it has symmetries as rotating it 90 degrees along some plane. What are all the possible symmetries we could get like this?*

Problem 12 (Putnam 2007 A5)**.** *Let G be a finite group that has exactly n elements of order p. Show that $n = 0$ or n divides $p + 1$.*