MATH 369 Fall 2025 - Class Notes

10/22/2025

Scribe: Ian Thomas

Summary: We discuss the last topics of **Chapter 3.8**, including simple groups, the fundamental homomorphism theorem, explore some homomorphisms, and start the beginning of **Chapter 4**.

- If $\phi : G \to H$ is a homomorphism, then $G/\phi \cong Im(\phi)$.

Theorem 1. ***(Fundamental Homomorphism Theorem)*** *If ϕ is a homomorphism $\phi : G \to H$, then $G/ker(\phi) \cong Im(\phi)$.*

Proof. Not given. □

- What is the center of $GL_n(F)$?
- $Z(GL_n(F)) = \{kI_n : k \in F^x\}$.
- **Definition.** $GL_n(F)/Z(GL_n(F))$ is the group where matrices are equivalent if they are constant multiples of each other. This is called $PGL_n(F)$, the projective linear group.
- $PSL_n(F) = SL_n(F)/Z(SL_n(F))$
- $|GL_2(\mathbb{Z}_3)| = ?$

With a 2x2 matrix, $a, b, c, d \in \mathbb{Z}_3$, we have $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. (a, b): 8 possibilities, then (c, d): 6 possibilities. so $|GL_2(\mathbb{Z}_3)| = 6 \times 8 = 48$.

- $det : GL_2(\mathbb{Z}_3) \to \mathbb{Z}_3^\times$ is a homomorphism.
- $ker(det) = SL_2(\mathbb{Z}_3)$, matrices with $det = 1$.
- Then $GL_2(\mathbb{Z}_3)/ker(det) \cong \mathbb{Z}_3^\times$. Since $|\mathbb{Z}_3^\times| = 2$, $[GL_2(\mathbb{Z}_3) : SL_2(\mathbb{Z}_3)]$, $|SL_2(\mathbb{Z}_3)| = \frac{48}{2} = 24$.
- What about $PGL_n(\mathbb{Z}_3) = GL_n(\mathbb{Z}_3)/Z(GL_n(\mathbb{Z}_3))$?
- $|PGL_n(\mathbb{Z}_3)| = 24$. Using SageMath, we find that $SL_2(\mathbb{Z}_3) \ncong PGL(\mathbb{Z}_3)$.
- **Definition.** A group is called simple if it doesn't have any nontrivial normal subgroups.

- Classification of all finite simple groups: Every finite simple group is part of 18 infinite families or one of the 26 "sporadic" groups that aren't part of these families.
- One of the largest of the sporadic groups is called the Monster Group. $|M| \approx 10^{53}$
- **Some Infinite Families:**

1. $\mathbb{Z}_p$, where p is prime
2. A_n, $n > 4$
3. $PSL_n(\mathbb{Z}_p)$, "for most n and p"

- **Definition.** A field is a set F that has two identity elements, called 0 and 1, ($0 \neq 1$), and two operations (usually denoted $+, \times$) such that $(F, +)$ is an abelian group. $(F \backslash \{0\}, x)$ is an abelian group and $a \times (b + c) = a \times b + a \times c, \forall a, b, \in F$ (distributive property).
- Some examples include $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Theorem 2. ***(Properties of Fields)*** *Let F be a field. Then*
1. $a \times 0 = 0, \forall a \in F$
2. if $ab = 0$, then $a = 0$ or $b = 0$
3. Cancellation property for multiplication: if $ac = ad$ and $a = 0$, then $c = d$

Proof. (1) By the distributive law, $a(0 + 0) = a \times 0 + a \times 0 = a \times 0$. Cancel out $a \times 0$ from both sides, then $0 = a \times 0$. Proofs for (2) and (3) follow from results about groups. □

- The requirement that + be commutative is redundant.
- The multiplication operation isn't guaranteed to be abelian.
- If a structure satisfies all requirements of a field except abelian multiplication, we call it a division ring.
- If F is any field, we can define $F[x]$ as the set of all polynomials whose coefficients are in F.
- **Example.** $\mathbb{Z}_3[x]$, polynomials with coefficients mod 3. $f(x) = x^2 + 2x + 1$, $g(x) = 2x^2 + x + 2$, $f(x) + g(x) = 0$