Dillan Marroquin
MATH 331.1001
Scribing Week 3
Due. 13 September 2021

Lecture 6

- $[k] \cdot [l] = [kl]$ is well-defined on $\mathbb{Z}/_n$ with respect to choice of n.
- Unlike $(\mathbb{Z} - \{0\}, \cdot, [1])$, $(\mathbb{Z}/_n - \{0\}, \cdot, [1])$ is NOT necessarily a monoid!

  Ex. $\mathbb{Z}/_4 - \{[0]\} \ni [2]$, but $[2] \cdot [2] = [0] \notin \mathbb{Z}/_4 - \{[0]\}$.

  Ex. $\mathbb{Z}/_3 - \{[0]\} := ([1], [2])$ and $[2] \cdot [2] = [1]$. This is stronger than a monoid; it's a group! (This is actually an "avatar" of the cyclic group of order 2)

- **Q: What's going on??**

Congruence and gcd

Lemma (6.1)**.** Let $n > 1$. If $k \equiv l \pmod n$ and $\gcd(k, n) = 1$, then $\gcd(l, n) = 1$.

Theorem (6.2)**.** Let $n > 1$. Define $\mathbb{Z}^\times/_n := \{[k] \in \mathbb{Z}/_n - \{[0]\} | \gcd(k, n) = 1\}$. Then $(\mathbb{Z}^\times/_n, \cdot, [1])$ is an abelian group called the **Group of Units mod n**.

Proof.

1. If $[k], [l] \in \mathbb{Z}^\times/_n$, then $[kl] \in \mathbb{Z}^\times/_n$ by Lem 6.3. Hence, $\cdot$ is a well-defined binary operator.
2. (Check Group Axioms):
   (a) Associativity (easy)
   (b) Left/Right Identity (easy)
   (c) Left/Right Inverse: Let $[a] \in \mathbb{Z}^\times/_n$. WTS $\exists [u] \in \mathbb{Z}^\times/_n$ such that $[a][u] = [1] = [u][a]$. Well, $\exists u, v \in \mathbb{Z}$ such that $au + nv = 1 \implies ua + nv = 1 \implies \gcd(u, n) = 1 \implies [u] \in \mathbb{Z}^\times/_n$. Moreover, $au + nv = 1 \implies n | au - 1$. Therefore, $[au] = [1]$. Hence, $[u]$ is the inverse of $[a]$. Similar proof gives $[u] \cdot [a] = [1]$.
3. Show abelian: $\forall [a], [b] \in \mathbb{Z}^\times/_n$, $[a] \cdot [b] = [b] \cdot [a]$. This is obvious due to commutativity of integers.

$\square$

Remark.

1. $\mathbb{Z}^\times/_n$ is well-defined by Lem 6.1.
2. We are "discarding" elements from $\mathbb{Z}^\times/_n - \{[0]\}$ to get a group.

Lemma (6.3)**.** Let $a, b \in \mathbb{Z}$ with $n < 1$. If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

Proof. There exist $u, u', v, v' \in \mathbb{Z}$ such that $au + nv = 1$ and $bu' + nv' = 1$. Therefore $(au + nv)(bu' + nv') = 1 \implies ab(uu') + n(\cdots) = 1$. Thus $\gcd(ab, n) = 1$ by Thm 2.2. $\square$

Corollary (6.4)**.** Let $p \in \mathbb{Z}$ be prime.

1. $\mathbb{Z}^\times/_n = \mathbb{Z}/_p - \{[0]\} = \{[1], [2], \dots, [p-1]\}$.
2. Every non-0 element of $\mathbb{Z}/_p$ has a multiplicative inverse.

Comparing Groups

Definition (6.5)**.** The **order $|G|$** of a group G is the cardinality of G as a set. G is **finite** iff $|G| < \infty$.
e.g. $|\mathbb{Z}/_n| = n$, $|\mathbb{Z}| = \infty$, $|GL_2(\mathbb{Z}/_p)| = (p^2-1)(p^2-p)$

Definition (6.6)**.** Let $(G, *_G, e_G)$ and $(H, *_H, e_H)$ be groups. A **group homomorphism** between G and H is a function $\rho : G \to H$ such that $\forall a, b \in G$, $\rho(a *_G b) = \rho(a) *_H \rho(b)$.

Lecture 7

Definition. A function $\rho : G \to H$ is **group isomorphic** iff ρ is a bijection and also a homomorphism.
We say G, H are **isomorphic** iff there exists a group isomorphism $\rho : G \to H$. We say $G \cong H$.

Ex (Basic Examples)**.**

1. Let G be a group. Then $\mathrm{id}_G : G \to G$ is a group isomorphism.
2. Let $n \in \mathbb{Z}$. Define $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\}$. Define $\rho : n\mathbb{Z} \to \mathbb{Z}$, $\rho(na) := na$.
   Observe that ρ is a homomorphism, but not a group isomorphism since ρ is not surjective.
3. Let $\mathbb{R}^\times := \mathbb{R} - \{0\}$, where $(\mathbb{R}^\times, \cdot, 1)$ is a group. Then $\det : GL_2 \to \mathbb{R}^\times$.
   Observe that this is a homomorphism, but not an isomorphism since it is not injective.
4. Let $n > 1$ and $\pi : \mathbb{Z} \to \mathbb{Z}/_n$, $\pi(a) := [a]$.
   This is a group homomorphism, but not an isomorphism (not injective).

Ex (Non-Examples)**.** Let $f, g : \mathbb{Z} \to \mathbb{Z}$.
Define $f(a) := a + 1$. This is not a homomorphism: $f(a+b) = a+b+1 \neq a+b+2 = f(a)+f(b)$.
Define $g(a) := a^2$. This is also not a homomorphism: $g(a+b) = a^2 + 2ab + b^2 \neq a^2 + b^2 = g(a) + g(b)$.

Abstract Properties of Group Homomorphisms

Proposition (7.1)**.** Let $(G, *_G, e_G)$ and $(H, *_H, e_H)$ be groups. Let $\rho : G \to H$ be a group homomorphism.

i. $\rho(e_G) = e_H$.
ii. $\forall g \in G$, if g^{-1} is the inverse of g, then $\rho(g^{-1})$ is the inverse of $\rho(g) \in H$.

Proposition (7.2)**.** If $\rho : G \to H$ for G, H groups is a group isomorphism, then

i. $|G| = |H|$.
ii. G is abelian iff H is abelian.