Lecture 6

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

  Example. $\mathbb{Z}/n4-\{[0]\}\ni[2]$, but $[2]\cdot[2]=[0]\notin\mathbb{Z}/n4-\{[0]\}$.

  Example. $\mathbb{Z}/n3-\{[0]\}:=([1],[2])$ 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 $(\mathbb{Z}/n)^{\times}n:=\{[k]\in\mathbb{Z}/nn-\{[0]\}|\gcd(k,n)=1\}$. Then $((\mathbb{Z}/n)^{\times}n,\cdot,[1])$ is an abelian group called the **Group of Units mod n**.

Proof.

1. If $[k],[l]\in(\mathbb{Z}/n)^{\times}n$, then $[kl]\in(\mathbb{Z}/n)^{\times}n$ 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 $[a]\in(\mathbb{Z}/n)^{\times}n$. WTS $\exists[u]\in(\mathbb{Z}/n)^{\times}n$ such that $[a][u]=[1]=[u][a]$. Well, $\exists u,v\in\mathbb{Z}$ such that $au+nv=1\implies ua+nv=1\implies\gcd(u,n)=1\implies[u]\in(\mathbb{Z}/n)^{\times}n$. 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: $\forall[a],[b]\in(\mathbb{Z}/n)^{\times}n$, $[a]\cdot[b]=[b]\cdot[a]$. This is obvious due to commutativity of integers.

■

Remark.

1. $(\mathbb{Z}/n)^{\times}n$ is well-defined by Lem 6.1.
2. We are "discarding" elements from $(\mathbb{Z}/n)^{\times}n-\{[0]\}$ 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. ■

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

1. $(\mathbb{Z}/n)^{\times}n=\mathbb{Z}/np-\{[0]\}=\{[1],[2],\dots,[p-1]\}$.
2. Every non-0 element of $\mathbb{Z}/np$ 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. $|\mathbb{Z}/nn|=n$, $|\mathbb{Z}|=\infty$, $|GL_2(\mathbb{Z}/np)|=(p^2-1)(p^2-p)$

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 $G \cong H$.

Example (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).

Example (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.

Lecture 8

Definition (8.1)**.** Let $(G, *_G, e_G)$ be a group. A **subgroup** of G is a subset $H \subseteq G$ (sometimes denoted $H \leq G$) such that

i) $e_g \in H$.

ii) $\forall h, h' \in H$, $h *_G h' \in H$.

iii) $\forall h \in H$, $h^{-1} \in H$.

Remark. If $H \leq G$, then $(H, *_G, e_G)$ is a group.

Examples/Non-Examples

1. For any $n \in \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$.
2. Let $2\mathbb{Z} + 1 := \{2k + 1 | k \in \mathbb{Z}\}$. This is NOT a subgroup since $e = 0 \notin 2\mathbb{Z} + 1$.
3. Let $G = \mathbb{Z}/n4$, $H := \{[0], [2]\}$. Indeed, H is a subgroup of G.
4. Let $n > 1$. Define $SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) | \det A = 1\}$. $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.
   Observe that this is easy to prove:
   For i), $\det(I_n) = 1$, therefore $I_n \in SL_n(\mathbb{R})$.
   For ii), let $A, B \in SL_n(\mathbb{R})$. Then $\det(AB) = \det A \cdot \det B = 1 \cdot 1 = 1$.
   For iii), let $A \in SL_n(\mathbb{R})$. To show $A^{-1} \in SL_n(\mathbb{R})$, observe that $\det(AA^{-1}) = \det A \cdot \det(A^{-1}) = \det(A^{-1})$. But $\det(AA^{-1}) = \det(I_n) = 1$, therefore $\det(A^{-1}) = 1$.

5. Let $H := \{A \in GL(n(\mathbb{R}) | \det A = -1\}$. Observe that $H \not\leq GL_n(\mathbb{R})$ since, for one, $I_n \notin H$.

Remark.

1. Every group G has at least 1 subgroup: the trivial group $\{e_G\}$.
2. If $|G| > 1$, then G has at least 2 subgroups: $\{e_G\}$ and G.

Definition (8.2)**.**

1. Let H be a subgroup of G. Then...
   i) H is **proper** iff $H \subset G$, i.e. $H \neq G$.
   ii) H is **non-trivial** iff $H \neq \{e_G\}$.
2. An abelian group G is **simple** iff it has no non-trivial proper subgroup.

- From now on, $(G, *_G, e_G)$ will be written as G, e_G will be e, $a *_G b$ will be ab, and $a *_G a *_G \cdots *_G a$ will be a^n.
- If G is abelian, $a *_g B$ is often written as $a + b$, $a *_G a *_G \cdots *_G a$ is written na, and a^{-1} is written $-a$.

Here is a useful tool for proving a group is a subgroup:

Proposition (8.3)**.** Let G be a group, and $H \subseteq G$ a subset. Then H is a subgroup iff $H \neq \emptyset$ and $\forall a, b \in H$, $ab^{-1} \in H$.

Proposition (8.4)**.** If $H, K \subseteq G$ are subgroups, then $H \cap K \subseteq G$ is also a subgroup.

Lecture 9

Let G be a finite group. How many subgroups does G have?

- If $|G| = n$, then G has 2^n subsets.
- In particular, G has subsets of cardinality $0, 2, \ldots, n$, but not all of these subsets will be subgroups!

Generalization of $\equiv \pmod{n}$

- Let G be a group, $H \subseteq G$ a subgroup. H defines a relation on G: for all $x, y \in G$, $x \sim_H y$ iff $x^{-1}y \in H$.

Proposition (9.1)**.** $\sim_H$ is an equivalence relation.

Definition (9.2)**.** The equivalence classes for $\sim_H$ are the **left cosets** of H in G. $G/_H$ is the set of left cosets. Define $[G : H] := |G/_H|$ to be the **index** of H in G (H has finite if $[G : H] < \infty$).

Example.

1. Let $G = \mathbb{Z}$, $n > 1$, $H = n\mathbb{Z}$. Then

$$\begin{aligned} a \sim_H b &\iff -a + b \in H \\ &\iff n | b - a \\ &\iff a \equiv b \pmod{n}. \end{aligned}$$

2. $\mathbb{Z}/_n\mathbb{Z} := \{[0], [1], \ldots, [n-1]\}$ (the set of left cosets).
3. $[\mathbb{Z} : n\mathbb{Z}] = n$.

Remark.

1. H can have finite index even if G, H have infinite order.
2. In general, $G/_H$ will not be a group.

Characterization of Left Coset

Proposition (9.3)**.** Let $H \subseteq G$ be a subgroup, $x \in G$, $[x]$ be the left coset represented by x, and define $xH := \{xh | h \in H\}$. Then $[x] = xH$.

Corollary (9.4)**.**

1. For all $x, y \in G$, we have $xH = yH$ iff $x^{-1}y \in H$.
2. If $y \in H$, then $yH = xH$.
3. For all $h \in H$, $hH = H$, i.e. $eH = H$.

Lecture 10

Remark. If $x \in G$, $x \notin H$, then xH is only a subset of G, not a subspace!
Why? If it were a subspace, then $e \in xH$ and so $\exists h \in H$ such that $e = xh$. Then $h^{-1} = xhh^{-1} \implies x = h^{-1} \in H$. Contradiction.

Proposition (10.1)**.** Let $H \subseteq G$ be a subspace, $x \in G$. Then the set-theoretic function $f : H \to xH$, $f(h) := xh$ is a bijection. In particular, $|xH| = |H|$.

Theorem (10.2 Lagrange)**.** Let G be a finite group, $H \subseteq G$ be a subgroup. Then $|G| = [G : H]|H|$. In particular, the order of H must divide the order of G.

Simple Remarks about Equivalence Classes

- Let S be a finite set, $\sim$ be an equivalence relation on S. Denote $S/\sim$ to be the set of equivalence classes on S.
- Choose a labeling for elements of $S = \{s_1, s_2, \ldots, s_n\}$.
  1. Each equivalence class $[s_i]$ is a finite subset and so is $S/\sim := \{[s_i] | i = 1, \ldots, n\}$.
  2. We may have $[s_i] = [s_j]$ even if $s_i \neq s_j$. So let m equal the number of distinct equivalence classes. Then $|S/\sim| = m$ and we can write $S/\sim = \{[s_{j_1}], [s_{j_2}], \ldots, [s_{j_m}]\}$.
  3. Prop. 5.1 implies that $S = \bigcup_{s_i \in S} [s_i]$. Hence $S = \bigcup_{k=1}^{m} [s_{j_k}]$.
  4. If $k \neq k'$, then $[s_{j_k}] \neq [s_{j'_k}]$. Therefore $|s_{j_k} \cup s_{j'_k}| = |s_{j_k}| + |s_{j'_k}|$.

Proof (Lagrange). Let $n = |G|$ and label the elements of $G = \{g_1, \ldots, g_2\}$. Let m be the number of distinct left cosets of H (e.g. $g_{i_1}H, g_{i_2}H, \ldots, g_{i_m}H$). This implies that $[G : H] = m$. Then $G = g_{i_1}H \cup g_{i_2}H \cup \cdots \cup g_{i_m}H$. Remark 4 implies that $|G| = |g_{i_1}H| + |g_{i_2}H| + \cdots + |g_{i_m}H|$ and Prop 10.1 implies $|G| = |H| + |H| + \cdots + |H|$ (m times) which equals $m|H|$ and thus $|G| = [G : H]|H|$. ∎

Corollary (10.3)**.** If $|G| = p$ prime, then G has no non-trivial proper subgroups. In particular, the only subgroup of $\mathbb{Z}/p$ are $\{[0]\}$ and $\mathbb{Z}/p$.

Lecture 11

Finitely Generated Groups

Motivation: In linear algebra, to describe every vector in $\mathbb{R}^2$, you only need 2 basis vectors along with a scalar (e.g. we can write $\begin{bmatrix} a \\ b \end{bmatrix} = a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = a\vec{e_1} + b\vec{e_2}$.

For a group G, we can sometimes find a finite subset $\{x_2, \ldots, x_n\} \subseteq G$ such that $\forall g \in G$, $\exists \{x_{i_1}, \ldots, x_{i_k}\} \subseteq \{x_1, \ldots, x_n\}$ and $n_1, \ldots, n_k \in \mathbb{Z}$ such that $g = x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k}$.
In this case, we say G is **finitely generated** and that $\{x_1, \ldots, x_n\}$ is a set of **generators** of G and we write $G = \langle x_1, \ldots, x_n \rangle$.

If G is Abelian and we're using additive notation, then we write elements of $G = \langle x_1, \ldots, x_n \rangle$ as $g = n_1 x_{i_1} + \cdots + n_k x_{i_k}$.

WARNING: The analogy between bases for a vector space and generators for a group is not perfect. Notions of linear independence, scalar multiples, and dimension do not make sense for groups in general.

Examples of Finitely Generated Groups

1. The abstract cyclic group of order 2: $G = \{e, \tau\}$ is finitely generated.
   We have $G = \langle \tau \rangle$ because $\tau = \tau^1$ and $e = \tau^0 = \tau^2$.

2. The Klein 4-group $V = \{e, a, b, c\}$ is finitely generated.
   We have $G = \langle a, b \rangle$ because $e = a^0 = b^0$, $a = a^1$, $b = b^1$, and $c = a^1 b^1$.

3. Any finite group G is finitely generated because $G = \langle G \rangle$.

Remark. If $|G| = \infty$, then it can be finitely generated.

4. The group $(\mathbb{Z}, +, 0)$ is finitely generated.
   We have $\mathbb{Z} = \langle 1 \rangle$ because $\forall n \in \mathbb{Z}$, $n = n \cdot 1$. (Note that $\mathbb{Z} = \langle -1 \rangle$ also!)

5. The group $\mathbb{Z}/n$ is finitely generated.
   Just like for $\mathbb{Z}$, we have $\mathbb{Z}/n = \langle [1] \rangle$.

Proposition (11.1)**.** Let $n > 1$. Then $\mathbb{Z}/n = \langle [a] \rangle$ iff $\gcd(a, n) = 1$. Particularly, the elements of the group of units $(\mathbb{Z}/n)^\times$ are precisely the set of all possible generators!

Example (Non-Abelian Example)**.** Let $S_3 := \{f : 1,2,3 \to 1,2,3 | f \text{ is bijective}\}$ where the group operation is function composition. We can write $f \in S_3$ as a table:

$$f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

with the 6 elements of S_3 being:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

One can check that $S_3 = \langle \sigma, \tau \rangle$, where $\sigma = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right]$ and $\tau = \left[\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right]$.
Indeed, $S_3 = \{e = \sigma^0 \tau^0, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$.

Example (Non-Example)**.** Any group that is not finitely generated must be infinite.

Proposition (11.2)**.** The group $(\mathbb{Q}, +, 0)$ is NOT finitely generated.

Lecture 12

Cyclic Groups

i.e. groups that can be generated by 1 element.

Lemma (12.1)**.**

1. Let G be a subgroup and $a \in G$. Then $\forall k, l \in \mathbb{Z}$, $a^k \cdot a^l = a^{k+l}$.

2. Let $(G, +, 0)$ be an Abelian group and let $a \in G$. Then

   i. $\forall k, l \in \mathbb{Z}$, $ka + la = (k + l)a$ and
   ii. $\forall k, l \in \mathbb{Z}$, $l(ka) = lka$.

Proposition (12.2)**.** Let G be a group and $a \in G$.

1. The subset $\langle a \rangle := \{a^k | k \in \mathbb{Z}\} = \{\ldots, a^{-1}, a^0, a^1, \ldots\}$ is a subgroup of G called the **cyclic subgroup** generated by a.

2. If $H \le G$ is any subgroup of G containing $a \in H$, then $\langle a \rangle \le H$. That is, a is the "smallest" subgroup of G containing a.

Definition (12.3)**.** A group is **cyclic** iff $a \in G$ such that $G = \langle a \rangle$.

Examples of Cyclic Groups/Subgroups

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ is cyclic.
2. Let $n > 1$. $n\mathbb{Z} := \{nk | k \in \mathbb{Z}\} = \langle n \rangle$ is a cyclic subgroup of $\mathbb{Z}$.
3. The trivial group $\{e\} = \langle e \rangle$ is cyclic.
4. The abstract cyclic group $G = \{e, \tau\} = \langle \tau \rangle$ is obviously cyclic.
5. $\mathbb{Z}/n = \langle [1] \rangle$.
6. Let $\mathbb{R}^\times := (\mathbb{R} - \{0\}, \cdot, 1)$. Let $H = \{1, -1\}$. Then $H = \langle 1 \rangle$.
7. Let $\mathbb{C}^\times := (\mathbb{C} - \{0\}, \cdot, 1)$ and let $H = \{1, i, -1, -i\}$. Then $H = \langle i \rangle$.

Definition (12.4)**.** Let G be a group, $a \in G$. The **order of a, $|a|$**, is the smallest positive integer such that $a^n = e$. If no such integer exists, then $|a| = \infty$.

Proposition (12.5)**.** Let G be a group, $a \in G$. If $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. In particular, $|\langle a \rangle| = |a|$.

Corollary (12.6)**.** Let G be a finite group. Then...

1. Every element of G has finite order and
2. $\forall a \in G$, $|a| \big| |G|$.

Lecture 13

Classifying Cyclic Groups

Goal: To show that every cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n$ (for a particular n).

Question: Given a group G, can we determine if G is cyclic?
Answer: This is hard to answer in general.

Theorem (13.1)**.** If $|G| = p$ for p prime, then G is cyclic. In particular, $\forall a \in G - \{e\}$, $G = \langle a \rangle$.

Abstract Properties of Cyclic Groups

Idea: If G does NOT have all of these following properties, then G cannot be cyclic. (Note that the converse is M E G A false!)

Proposition (13.2)**.** Every cyclic group is abelian.

Theorem (13.3)**.** Every proper subgroup of a cyclic group is cyclic.

Remark (13.4). The converse of Theorem 13.3 is false.

Lecture 14

The converse of Theorem 13.3 from last lecture is NOT true: If every proper subgroup G is cyclic, it is not guaranteed that G is cyclic. Here are two counter-examples:

1. Consider $S_3 := \{\text{bijections from } \{1,2,3\} \to \{1,2,3\}\}$. The order of S_3 is 6, so by Lagrange's Theorem any proper subgroup of S_3 has order $1, 2$, or 3. For a subgroup $H \leq S_3$ with $|H| = 1$, then $H = \{e\} = \langle e \rangle$ and is cyclic.
   By Theorem 13.1, if $|H| = 2$ or 3, H is cyclic. Therefore every proper subgroup is cyclic, but obviously S_3 is not cyclic since it is not abelian.
2. Now consider $G = \mathbb{Z}/3 \times \mathbb{Z}/3$ with $([a_1], [b_1]) + ([a_2], [b_2]) = ([a_1 + a_2], [b_1 + b_2])$. Then $|G| = 9$. The same argument as above implies that every proper subgroup is cyclic because it must have order 1 or 3. Note G is abelian. We can check by hand that every element of G has order 1 or 3, NOT 9. Therefore G is not cyclic. For example, $3([a], [b]) = (3[a], 3[b]) = ([0], [0])$.

Corollary (14.1)**.**

1. Let $H \leq \mathbb{Z} = \langle 1 \rangle$ be a subgroup. Then $\exists m > 0$ such that $H = \langle m \rangle = m\mathbb{Z}$.
2. If $H \leq \mathbb{Z}/m$ is a subgroup, then $\exists [m] \in \mathbb{Z}/n$ such that $H = \langle [m] \rangle = \{[0], [m], [2m], \ldots\}$.

Finding the Order of a Subgroup of a Cyclic Group

Theorem (14.2)**.** Let $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ be a finite cyclic group of order n. Let $a^k \in G$. Then $|a^k| = \frac{n}{\gcd(n,k)}$.

Lemma (14.3)**.** If $G = \langle a \rangle$ has order n and $l \in \mathbb{Z}$, $l > 0$ such that $a^l = e$, then $n|l$.

Lemma (14.4)**.** Given $k, n \in \mathbb{Z} \setminus \{0\}$, let m_k, m_n be unique integers such that $k = dm_k$ and $n = dm_n$, where $d = \gcd(n,k)$. Then $\gcd(m_k, m_n) = 1$.

Lecture 15

Converse to Lagrange's Theorem for Cyclic Groups

Corollary (15.1)**.** If $G = \langle a \rangle$ is a cyclic group of order n and l is a positive divisor of n, then there exists a subgroup $H \leq G$ with $|H| = l$.

Classification of Cyclic Groups

Recall: Let G, H be groups. A function $\Phi : G \to H$ is a group homomorphism iff $\forall x, y \in G$, $\Phi(xy) = \Phi(x)\Phi(y)$. Also, Φ is an isomorphism iff it is bijective and a homomorphism.

Remark. "$\cong$" gives an equivalence relation on the "set" of group implies $G \cong H$ iff $H \cong G$.

Theorem (15.2)**.** If $G = \langle a \rangle$ is a cyclic group of infinite order, then $G \cong \mathbb{Z}$.

Proof. By the above Remark, it suffices to construct a group isomorphism $\Phi : \mathbb{Z} \to G$. Observe that $G = \{a^k | k \in \mathbb{Z}\}$. Define $\Phi(k) := a^k$. To show Φ is a group homomorphism, let $k, l \in \mathbb{Z}$. Then $\Phi(k+l) = a^{k+l} = a^k a^l = \Phi(k)\Phi(l)$.
To show Φ is a bijection, we first prove surjectivity. Consider the image of Φ: $\Phi(\mathbb{Z}) = \{\Phi(k) | k \in \mathbb{Z}\} = \{a^k | k \in \mathbb{Z}\}$. But $\{a^k | k \in \mathbb{Z}\} = G$, so Φ is surjective.
To show Φ is injective, suppose $\Phi(k) = \Phi(l)$. Then $a^k = a^l$ in G which implies $a^k a^l = e$ and thus $a^{k-l} = e$. Since a has infinite order, $a^{k-l} = e$ iff $k - l = 0$. Therefore $k = l$ and Φ is injective. ∎

Theorem (15.3)**.** If $G = \langle a \rangle$ is cyclic order n, then $G \cong \mathbb{Z}/n$.

Looking Ahead: Getting Subgroups from Group Homomorphisms

Definition (15.4)**.** Let $\Phi : G \to H$ be a group homomorphism.

1. The **image** of Φ is the subset of H where $\mathrm{im}\Phi = \{\Phi(x) | x \in G\}$.
2. The **kernel** of Φ is the subset of G where $\ker\Phi = \{x \in G | \Phi(x) = e_H\}$.

Lecture 16

Proposition (16.1)**.** Let φ be a group homomorphism.

1. $\mathrm{im}\varphi$ is a subgroup of H.
2. $\ker\varphi$ is a subgroup of G.

Proof. (1.) Use Proposition 8.3, which tells how to find a subgroup, and Proposition 7.1 (which states that for $\varphi : G \to H$, $\varphi(e_G) = e_H$ and $\varphi(x^{-1}) = \varphi(x)^{-1}\ \forall x \in G$). Since $\varphi(e_G) = e_H$, we have $e_H \in \text{im}\varphi \neq \emptyset$ and so $\text{im}\varphi$ is not empty. Let $a, b \in \text{im}\varphi$. We want to show that $ab^{-1} \in \text{im}\varphi$. By definition of $\text{im}\varphi$, $\exists x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Then $ab^{-1} = \varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1})$ by definition of group homomorphism. Thus, $ab^{-1} \in \text{im}\varphi$.
(2.) We will use the same previous propositions. By Proposition 7.1, $\varphi(e_G) = e_H$ which implies that $e_H \in \ker\varphi \neq \emptyset$. Let $x, y \in \ker\varphi$. We want to show $xy^{-1} \in \ker\varphi$. Note that $\varphi(y) = e_H$ which implies $\varphi(y)^{-1} = e_H$. Then by definition of group homomorphism, $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1})$, and since $x \in \ker\varphi$, $\varphi(x)\varphi(y^{-1}) = e_H\varphi(y^{-1}) = e_H^2 = e_H$. Thus $\varphi(xy^{-1}) = e_H \in \ker\varphi$. ∎

Lecture 17

Proposition (17.1)**.** Let $\varphi : G \to H$ be a group homomorphism. Then φ is injective iff $\ker\varphi = \{e_G\}$, i.e. iff $\ker\varphi$ is the trivial subgroup.

Proof. Suppose φ is injective. We want to show $x = e_G$. Let $x \in \ker\varphi$. Then $\varphi(x) = e_H$ by definition, and by Proposition 7.1, $\varphi(e_G) = e_H$. Since φ is injective, $\varphi(x) = e_H$ and $\varphi(e_G) = e_H$ implies $e_G = x$ and thus $\ker\varphi = \{e_G\}$.
Conversely, suppose $\ker\varphi = \{e_G\}$. Assume $\varphi(x) = \varphi(y)$. Then $\varphi(x)\varphi(y)^{-1} = e_H$. By Proposition 7.1, $\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1})$ and by definition of group homomorphism $= \varphi(xy^{-1}) = e_H$. Thus $xy^{-1} \in \ker\varphi$, but since $\ker\varphi = \{e_G\}$, $xy^{-1} = e_G$ and by multiplying each side by y on the right, we obtain $x = y$ as desired. ∎

Corollary (17.2)**.** Let $\varphi : G \to H$ be a group homomorphism. Then φ is a group isomorphism iff $\ker\varphi = \{e_G\}$ and $\text{im}\varphi = H$.

Normal Subgroups

(Which, by the way, the term ”normal” sucks!)

<u>**Idea:**</u> Recall given a subgroup $H \leq G$, we can define an equivalence relation on G, $x \sim_H y$, iff $x^{-1}y \in H$. The equivalence classes are the left cosets of H: $[x] = xH := \{xh | h \in H\}$. We denote the set of lefts cosets as $G/H = \{xH | x \in G\}$. Consider the groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Q}/\mathbb{Z}$.

Remark (17.3). In the above groups, G induces a group operation (and identity) on G/H such that the function $\pi : G \to G/H$, $x \mapsto [x] = xH$ is a group homomorphism!

Example. Let $G = S_3$, $H = \langle\sigma\rangle$, $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$. Note that $|G/H| = [G : H] = 2$ by Lagrange's Theorem.
Then $G/H = \{eH, \tau H\} = \{H, \tau H\}$ for $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$. The goal is to put a group structure on G/H as in Remark 17.3. That is, we want $xH \cdot yH \stackrel{?}{=} xyH$ and $e_{G/H} \stackrel{?}{=} e_{S_3}H = H$. This works! Verify by hand: e.g. $\tau H \cdot \tau H = \tau^2 H = eH = H$. $\tau H = \{\tau, \tau\sigma, \tau\sigma^2\} = \tau\sigma H$.

Example. Let $G = S_3$, $H = \langle\tau\rangle$. Then $G/H = \{H, \sigma H, \sigma^2 H\}$ (we can verify this is correct by hand). Again, we want to define a group operation on G/H. BUUUT it does not work!

Lecture 18

Example (Non-Example)**.** (Continuation from last lecture) Let $G = S_3$, $H = \langle\tau\rangle$, where $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ and $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$.
Then $G/H = \{eH = H, \sigma H, \sigma^2 H\}$ and $\sigma H = \{\sigma e = \sigma, \sigma\tau\}$.
If G/H is indeed a group, we must have that $\sigma H * \tau H = \sigma H$ and $\tau H * \sigma H = \sigma H$ because $\tau H = H$ is our identity element.

1. By definition of *, $\sigma H * \tau H = \sigma\tau H = \{\sigma\tau, \sigma\tau \circ \tau = \sigma\} = \sigma H$. Therefore, 1. is true.
   <u>**Note:**</u> $xH \cap yH \neq \emptyset$ implies $xH = yH$ because left cosets are equivalence classes of an equivalence relation.

2. $\tau H * \sigma H = \tau\sigma H = \{\tau\sigma, \tau\sigma\tau\}$ by definition of *. But $\tau\sigma \neq \sigma$ and $\tau\sigma \neq \sigma\tau$, therefore $\tau\sigma H \neq \sigma H$ and thus we conclude $G/H = S_3\langle\tau\rangle$ is not a group.

But what went wrong?? We will see that this happened because $\langle\tau\rangle$ is not a normal subgroup.

Definition (18.1)**.** A subgroup $H \leq G$ is **normal** iff for all $g \in G$, the set $gHg^{-1} := \{ghg^{-1} | h \in H\}$ is equal to H. We write $G \trianglelefteq H$

Remark. If $H \trianglelefteq G$, then

1. For all $g \in G$ and for all $h \in H$, $ghg^{-1} \in H$. i.e. $\exists h' \in H$ such that $ghg^{-1} = h'$ (since $gHg^{-1} \subseteq H$), but in general $h' \neq h$.
2. Let $h \in H$. Then $\forall g \in G, \exists h' \in H$ such that $h = gh'g^{-1}$ (since $H \subseteq gHg^{-1}$.

Proposition (18.2 USEFUL)**.** Let $H \leq G$ be a subgroup. Assume $\forall g \in G, \forall h \in H$, we have $ghg^{-1} \in H$. Then

1. $\forall g \in G, gHg^{-1} \leq H$ and
2. $\forall g \in G, H \leq gHg^{-1}$.

i.e. H is normal.

1st Examples/Non-Examples

Proposition (18.3)**.** Let G be abelian. Then every subgroup of G is normal.

Proof. Let H be a subgroup, $g \in G$, and let $h \in H$. Since G is abelian, $ghg^{-1} = hgg^{-1}$. Therefore, $ghg^{-1} = h \in H$. ■

Proposition (18.4)**.** A subgroup $H \leq G$ is normal iff $\forall x \in G, xH = Hx$.

Corollary (18.5)**.** If $H \leq G$ is a subgroup and $[G : H] = 2$, then H is normal.

Example. $H = \langle \sigma \rangle$ is normal in $G = S_3$ since $[S_3 : H] = 2$.

Example (Non-Example)**.** $H := \langle \tau \rangle$ is not normal in $G = S_3$. Observe that $\sigma\tau\sigma^{-1} \notin H$.

Lecture 19

Theorem (19.1)**.** Let $H \trianglelefteq G$ be a normal subgroup.

1. The set of left cosets G/H is a group with binary operation $xH * yH = xyH$ and identity element $e_{G/H} := e_G H = H$.
2. The group structure from 1. makes $\pi : G \to G/H$, $\pi(g) := gH$ a surjective group homomorphism.

Proof.

1. The main point is to check that the binary operation is well-defined (since all group axioms will follow immediately from those on G). Suppose $x'H = xH$ and $y'H = yH$. WTS $x'y'H = xyH$. The first two equalities imply $\exists h, \tilde{h} \in H$ such that $x' = xh$ and $y' = yh$. WTS $\exists h'$ such that $x'y' = xyh$. Consider $x'y' = xhy\tilde{h} = xehy\tilde{h} = xyy^{-1}hy\tilde{h}$. Since $H \trianglelefteq G$, $ghg^{-1} \in H$, where $g := y^{-1}$. Therefore $\exists h' \in H$ such that $y^{-1}hy = h'$ which implies that the RHS$= xyh'\tilde{h} \in xyH$. Thus $x'y' \in xyH$.
2. This is straightforward: $\pi(xy) = xyH = xH * yH = \pi(x) * \pi(y)$. This is surjective vacuously.

■

Basic Examples of Quotient Groups

Remark. Groups of the form G/H are called **Quotient/Factor Groups**.

Example. Let $G = S_3$, $H = \langle \sigma \rangle$. Note $G/H = \{H, \tau H\}$ is a group of order $[G : H] = 2$. So $G/H \cong \mathbb{Z}/2$ by theorem 15.2.

Proposition (19.2)**.** Let $\varphi : G \to G'$ be a group homomorphism. Then $\ker\varphi$ is a normal subgroup of G.

Remark. Proposition 19.2 implies that if $H \leq G$ is a subgroup and there exists a function $\varphi : G \to G'$ such that $H = \ker\varphi$, then $H \trianglelefteq G$.

Proposition (19.3)**.** Let $H \trianglelefteq G$ be a normal subgroup. Then the kernel of $\pi : G \to G/H$ is H.

Lecture 20

Notation: Let G be abelian, $H \leq G$ a subgroup. If we write G additively, then we write cosets of H as $a+H = aH$. We write the group operation in G/H as $x+H+y+H := (x+y)+H$.
i.e. $\mathbb{Z}/n$: $k+n\mathbb{Z}$ and for $\mathbb{Q}/\mathbb{Z}$: $\frac{a}{b}+\mathbb{Z}$.

Example of Analyzing G/H via Proposition 19.2/19.3

- Consider $\det : GL_2(\mathbb{R}) \to \mathbb{R}^\times$.
  $\ker(\det) = \{A \in GL_2 | \det A = 1\} := SL_2(\mathbb{R})$. Proposition 19.2 implies $\ker(\det) \trianglelefteq GL_2$.
  Note: SL_2 is not abelian.
- We will be analyzing $GL_2/SL_2 := \{ASL_2 | A \in SL_2\}$.
- We will also analyze left cosets:

Lemma (20.1)**.** Let $H \leq G$ be a subgroup. Then $xH = yH$ iff $x^{-1}y \in H$.

Proof. This will be #1 on PS 5. He tricked us! ∎

Observations:

1. By the above Lemma, $ASL_2 = BSL_2$ iff $A^{-1}B \in SL_2$ iff $\det(A^{-1}B) = 1$ iff $\det A^{-1} \det B = 1$ iff $\det A = \det B$.
2. $\forall A \in GL_2$, $ASL_2 = \begin{bmatrix} \det A & 0 \\ 0 & 1 \end{bmatrix} SL_2$ which implies that as a set, $GL_2/SL_2 := \left\{ \begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} SL_2 | r \in \mathbb{R} \setminus \{0\} \right\}$.
3. Note: $\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} SL_2 = \begin{bmatrix} r' & 0 \\ 0 & 1 \end{bmatrix} SL_2$ iff $r = r'$.

But what about the group operation? By definition,
$\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} SL_2 * \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix} SL_2 = \begin{bmatrix} rs & 0 \\ 0 & 1 \end{bmatrix} SL_2 = \begin{bmatrix} sr & 0 \\ 0 & 1 \end{bmatrix} SL_2 = \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix} SL_2 * \begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} SL_2$. Therefore, GL_2/SL_2 is abelian!
This is AMAZINGLY important because G and H are non-abelian, thus G, H being non-abelian does NOT imply that G/H is non-abelian.

Observation 1 implies that we have a well-defined function $\overline{\det} : GL_2/SL_2 \to \mathbb{R} \setminus \{0\}$, $\overline{\det}\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} SL_2 \right) := r = \det\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix} \right)$.
$\overline{\det}$ is a group homomorphism. Also, it is surjective since $\det : GL_2 \to \mathbb{R}^\times$ is surjective. It is also injective by Observation 3. Therefore, $\overline{\det}$ is a group isomorphism and thus $GL_2/SL_2 \cong \mathbb{R}^\times$.

1st Isomorphism for Groups

Theorem (20.2)**.** Let $\varphi : G \to G'$ be a group homomorphism. Then the function $\overline{\varphi} : G/\ker\varphi \to \mathrm{im}\varphi$, $\overline{\varphi}(x\ker\varphi) := \varphi(x)$ is a group isomorphism.

Proof. (See Paulin). ∎

Example. Let $\varphi : \mathbb{Z} \to S_3$, $\varphi(k) := \sigma^k$ be a group homomorphism such that $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Hence, $\mathrm{im}\varphi = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$. Then $\ker\varphi = \{k \in \mathbb{Z} | \sigma^k = e\}$. Lemma 14.3 says if $\sigma^k = e$, then $|\sigma| \big| k$ which implies $k \in 3\mathbb{Z}$. By Theorem 20.2, $\mathbb{Z}/3 \cong \langle \sigma \rangle$ on $\overline{\varphi}$.

Q: 2 subgroups from $\varphi : G \to H$: $\ker\varphi \leq G$ and $\mathrm{im}\varphi \leq H$. We've already seen that $\ker\varphi$ is always normal, but what about $\mathrm{im}\varphi$ in H??

Lecture 21

Q: Is the image of a group homomorphism $\varphi : G \to H$ a normal subgroup of H?
A: Nope! As an example, take $G = \mathbb{Z}$, $H = S_3$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then $\mathrm{im}\varphi = \{\varphi(k) | k \in \mathbb{Z}\} = \{\tau^k | k \in \mathbb{Z}\} = \langle \tau \rangle$. We know from past lectures that $\langle \tau \rangle \leq S_3$ is not a normal subgroup.

Permutation Groups

Definition (21.1). Let X be a set. The **permutation group of X** is the set $\Sigma(X) := \{f : X \to X | f \text{ is a bijection}\}$ with binary operator being function composition, $\circ$, and identity element $e(x) = x$, $\forall x \in X$.

Most important example: $X = \mathbb{n} = \{1, \ldots, n\}$, $n \geq 1$. Then $\Sigma(X) = S_n$ is the **symmetric group on n-letters (Sym$_\mathbf{n}$, $\Sigma_\mathbf{n}$)**.

Proposition (21.2). Let $X = \{x_1, \ldots, x_n\}$ be an n-element set. Then $\Sigma(X) \cong S_n$.

Permutation Group of a Group: $\Sigma(G)$

Remark. Paulin uses the idea of a "group action." This is important, but we'll ignore it.

Let G be a group. Then $\Sigma(G) := \{f : G \to G | f \text{ is a set-theoretic bijection}\}$.
Let $g \in G$. Define a function $L_g : G \to G$, $L_g(x) := gx$, $\forall x \in G$. Note that L_g is not a group homomorphism if $g \neq e_G$, but it is a bijection.

Example. Let $G = \mathbb{Z}$. Then $L_g(a) = g *_G a = a + n$ (translation by n).

Lemma (21.3). Let G, H be groups and let $\varphi : G \to H$ be a group homomorphism. If φ is injective, then φ induces a group isomorphism $G \cong \text{im}\varphi \leq H$.

Theorem (21.4 Cayley's Theorem). Let G be a group, $\Sigma(G)$ be the permutation group of the SET G. Let $\varphi : G \to \Sigma(G)$ be the function $\varphi(g) := L_g$. Then

1. φ is a group homomorphism and
2. φ induces a group isomorphism between G and the subgroup $\text{im}\varphi \leq \Sigma(G)$.

Corollary (21.5). Every finite group is isomorphic to a subgroup of S_n.

Lecture 22

Proof of Theorem 21.4.

1. Want to show $\forall g, g' \in G$, $\varphi(gg') = \varphi(g) \circ \varphi(g')$ i.e. we want to show $L_{gg'} = (L_g \circ L_{g'})(x)$. The left-hand side $= gg'x$ and the right-hand side $= L_g(L_{g'}(x)) = L_g(g'x) = gg'x$.
2. Suffices to show $\varphi : G \to \text{im}\varphi$ is injective since any function is surjective onto its image (Lemma 21.3). By Prop. 17.1, we want to show $\ker\varphi = \{e_G\}$. Suppose $g \in \ker\varphi$. Then $\varphi(g) = \text{id}_G$, i.e. $\forall x \in G$, $L_g(x) = \text{id}_G(x) = x$. Since $x \in G$, $x^{-1} \in G$. Therefore $gx = x$ implies $g = e_G$. Thus injective.

■

Corollary (21.5). Every finite group G of order n is isomorphic to a subgroup of $S_n = \Sigma(\{1, 2, \ldots, n\})$.

Structure of Symmetric Group S_n

S_n is B I G! $|S_n| = n!$, so it's too hard to write the elements of S_n as $\left(\begin{smallmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 6 & 1 & \cdots & 7 \end{smallmatrix}\right)$.

Definition (22.1). Let $i_1, i_2, \ldots, i_k$ be distinct elements of $\mathbb{n} = \{1, \ldots, n\}$ with $1 \leq k \leq n$. Then $(i_1, i_2, \ldots, i_k) \in S_n$ denotes the function $i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{k-1} \mapsto i_k, i_k \mapsto i_1$. Every other element of $\mathbb{n}$ gets mapped to itself. $(i_1, \ldots, i_k)$ is a **k-cycle**. 2-cycles are **transpositions**.

Example.

1. Our friends σ, $\tau \in S_3$, where $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$. ☺ In cycle notation we have $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 3)$
2. Let $\rho = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{smallmatrix}\right) \in S_4$. Then $\rho = (1\ 4\ 3\ 2)$.
3. $\text{id}_\mathbb{n} \in S_n$ and $\text{id}_\mathbb{n} = (1) = (2) = (3) = \cdots$.

Remark.

1. Example 3 shows there are multiple ways to express cycles- Ex 1: $\sigma = (3\ 1\ 2) = (2\ 3\ 1)$, $\tau = (2\ 3) = (3\ 2)$.

2. Without context, it's unclear where these cycles live. e.g. $(1\ 2\ 3)$ could be in S_3 or S_4 corresponding to $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

Proposition. Let $\sigma = (i_1\ i_2\ \dots\ i_k) \in S_n$ be a k-cycle. Then:

1. $|\sigma| = k$ and
2. $\sigma^{-1} = (i_k\ i_{k-1}\ \dots\ i_2\ i_1)$.

Lecture 23

Remark. This is important! Not every element in S_n is a cycle!

Example. $\eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$. Note that $|\eta| = 2$. Prop. 22.1(1) implies $\eta = (i_1\ i_2)$. So η leaves 2 elements of $\{1,2,3,4\}$ fixed, which is false.

Composition of Cycles: "Important" Group Operation in S_n into Cycle Notation

Example. 1. Let $\sigma = (1\ 3\ 5\ 2)$, $\tau = (2\ 5\ 6) \in S_6$. Then $\sigma \circ \tau = \sigma\tau = (1\ 3\ 5\ 2)(2\ 5\ 6) = (1\ 3\ 5\ 6)$.

2. Let $\sigma = (1\ 3\ 5\ 2)$, $\tau = (1\ 6\ 3\ 4) \in S_6$. Then $\sigma\tau = (1\ 3\ 5\ 2)(1\ 6\ 3\ 4) = (1\ 6\ 5\ 2)(3\ 4)$ which is NOT a cycle!

Observation: $\alpha = (1\ 6\ 5\ 2)$, $\beta = (3\ 4)$ commute: $\alpha\beta = \beta\alpha$.

Definition (23.1)**.** 2 cycles $(i_1\ i_2\ \dots\ i_r)$ and $(j_1\ j_2\ \dots\ j_s)$ are **disjoint** iff $\forall k = 1,\dots,r$, $i_k \neq j_l$, $\forall l = 1,\dots,s$.

Proposition (23.2)**.** If $\sigma, \tau \in S_n$ are disjoint cycles, $\sigma\tau = \tau\sigma$.

Proof. We want to show $\forall m \in \mathtt{n}$, $\sigma\tau(m) = \tau\sigma(m)$. Let $I := \{i_1,\dots,i_r\}$, $J := \{j_1,\dots,j_k\}$. Let $m \in \mathtt{n}$. We observe 3 different cases:
Case 1: $m \notin I$, $m \notin J$. By definition of cycle, $\tau(m) = m$ and $\sigma(m) = m$. Therefore $\sigma\tau(m) = m = \tau\sigma(m)$.
Case 2: $m \in I$. Consider $\sigma\tau(m)$. Since $m \in I$, $m \notin J$ and therefore $\tau(m) = m$ which implies $\sigma\tau(m) = \sigma(m)$. Consider $\tau\sigma(m)$. Then $\sigma(m) \in I$ which implies $\sigma(m) \notin J$ and therefore $\tau\sigma(m) = \sigma(m)$.
Case 3: $m \in J$. Same as Case 2, just swap the roles of I, J. ■

Remark. Let $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 3) \in S_3$. Then $\sigma\tau = (1\ 2\ 3)(2\ 3) = (1\ 2) \neq (1\ 3) = (2\ 3)(1\ 2\ 3) = \tau\sigma$.

Corollary (23.3)**.** Let $\alpha \in S_n$ be the product of disjoint cycles $\sigma_1, \sigma_2, \dots, \sigma_k \in S_n$. Then $|\sigma| = \operatorname{lcm}\{|\sigma_1|, |\sigma_2|, \dots, |\sigma_k|\}$.

Lecture 24

We will begin with a proof of Corollary 23.3 from last lecture...

Proof Cor 23.3. By Proposition 23.2, all σ commute with one another. Thus $\alpha^l = \sigma_1^l \sigma_2^l \cdots \sigma_k^l$ $\forall l \geq 1$. As $\{\sigma_i\}$ is disjoint for all i, σ_i^{-1} and $\sigma_{j\neq 1}^l$ are disjoint also. Then $\alpha^m = e$ iff $\sigma_i^m = e$ $\forall i = 1,\dots,k$. Lemma 14.2 implies $|\sigma_i| \big| m$. Thus $\alpha^m = e$ iff m is a multiple of $|\sigma_1|, |\sigma_2|, \dots, |\sigma_k|$. By definition of order, $|\alpha|$ must be the smallest such that $\alpha^m = e$, so $|\alpha^m| = e$, so $|\alpha| = \operatorname{lcm}\{|\sigma_i|\}_{i=1}^k$. ■

Generators of S_n

Here, we are looking for the set of elements of $\{\sigma_1, \dots, \sigma_n\} \subseteq S_n$ such that every element of S_n can be written as $\sigma_1^{k_1}, \dots, \sigma_n^{k_n}$ for $k_1, \dots, k_n \in \mathbb{Z}$.

Proposition (24.1)**.** Let $n \geq 2$ and $\sigma = (i_1 \dots i_k) \in S_n$ be a k-cycle. Then σ can be written as a product of transpositions. In particular, $\sigma = (i_1\ i_k)(i_1\ i_{k-1}) \dots (i_1\ i_2)$ (i.e. $k-1$ transpositions).

Remark (Ex 24.2)*.* Consider $\sigma = (1\ 2\ 3\ 4) \in S_4$. Then $(1\ 4)(1\ 3)(1\ 2) = (1\ 2\ 3\ 4)$. Note that $1 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, and $3 \mapsto 1 \mapsto 4$.
Note: Decompositions into transpositions are note unique! For example, $(1\ 2)(2\ 3)(1\ 2)(3\ 4)(1\ 2) = (1\ 2\ 3\ 4)$ as well.

Theorem (24.3)**.** Every non-identity element of S_n is uniquely (up to rearrangement) a product of disjoint cycles, each of length 2.

This is how we define our cycle notation: $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{smallmatrix}\right) \in S_6 = (1\ 3)(4\ 5\ 6)$.

Corollary (24.4)**.** For all $n \geq 2$, S_n is generated by the set of transpositions $\{(i\,j) \in S_n | 1 \leq i < j \leq n\}$.

Remark. We also know that S_3 is generated by $\sigma = (1\ 2\ 3)$ and $\tau = (2\ 3)$. We can also show that $S_{n>3}$ is generated by $\sigma = (1\ 2\ 3\ \ldots\ n-1\ n)(n-1\ n)$.

Lecture 25

Sign of Permutation

Definition (25.1)**.** Let $\sigma \in S_n$. We say σ is **even/odd** iff σ can be written as an even/odd number of transpositions. We write $\operatorname{sgn}(\sigma) := +1$ if σ is even or -1 if σ is odd.

Example. If $\sigma = (i_1\ i_2\ \ldots\ i_k) \in S_n$ is a k-cycle, then σ is even if k is odd, or odd if k is even.
Proposition 24.1 implies $\sigma = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)$.

Theorem (25.2)**.** A permutation can't be both odd and even. In particular, $\operatorname{sgn} : S_n \to \{\pm 1\}$ is well-defined.

Evidence for Theorem 25.2: Let $\vec{e_1}, \ldots, \vec{e_n}$ be a standard basis of $\mathbb{R}^n$. So $\vec{e_1} = [1\ 0\ 0\ \cdots\ 0], \vec{e_2} = [0\ 1\ 0\ \cdots\ 0], \ldots$. To each $\sigma \in S_n \mapsto n \times n$ matrix P_σ:
$P_\sigma := [\vec{e_{\sigma(1)}}, \vec{e_{\sigma(2)}}, \ldots, \vec{e_{\sigma(n)}}]$.

Example.

1. $S_2 = \{(1), (1\ 2)\}$. We have $(1) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $(1\ 2) \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
2. $\sigma = (1\ 2\ 3) \in S_3 \mapsto P_\sigma = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Note that $\det(P_\sigma) = 1 = \operatorname{sgn}(\sigma)$ since σ is a 3-cycle.

Fact: $S_n \to \mathrm{GL}_n(\mathbb{R})$ is a group homomorphism.

If an $n \times n$ matrix $A = [\vec{a_1}\ \vec{a_2} \ldots\ \vec{a_n}]$, then swapping any 2-columns changes the sign of the determinate.

Fact: $\operatorname{sgn}(\sigma) = \det(P_\sigma)$.

Lecture 26

Paulin Chapter 4: Rings!

Idea: Study objects like $(\mathbb{Z}, +, 0, *, 1)$, develop an abstract notion of primes and the fundamental theorem of arithmetic.

Definition (26.1)**.** A **ring** $(\mathbf{R}, +, \mathbf{0}, *, \mathbf{1})$ is a set R equipped with binary operators $+, * : R \times R \to R$ and elements $0, 1 \in R$ such that

1. $(R, +, 0)$ is an abelian group,
2. $(R, *, 1)$ is a monoid (i.e. a group where multiplicative inverses may not exist),
3. Left/Right distributive law holds: $\forall a, b, c \in R$, $(a+b)*c = a*c + b*c$ and $a*(b+c) = a*b + a*c$.

Notation: $ab := a*b$ and $\forall n \geq 0 \in Z$, $na := a + a \cdots + a$ (n times) and $a^n := a*a*\cdots*a$ (n times). Note that $na \neq a^n$ in general.

Definition (26.2)**.** A ring R is commutative iff $\forall a, b \in R$, $a*b = b*a$.

Basic Examples of Rings

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Commutative.
2. $(\mathbb{Z}/n, \overline{+}, \overline{0}, \overline{*}, \overline{1})$. Commutative.
3. The Zero Ring $R = \{0_R\}$, where $1_R = 0_R$. Commutative.
4. $M_n(\mathbb{R}) := \{n \times n$ matrices with entries in $\mathbb{R}\}$, $(M_n(\mathbb{R}), +, 0_n, *, I_n)$. Non-commutative for $n \geq 2$.
5. $\mathcal{C}([0,1]) := \{f : [0,1] \to \mathbb{R} | f$ is continuous$\}$. In this ring, $(f+g)(x) := f(x) + g(x)$, $(fg)(x) := f(x)g(x)$, $0(x) := 0 \in \mathbb{R}$, $1(x) := 1 \in \mathbb{R}\ \forall x \in [0,1]$.

Abstract Properties of Rings

Proposition (26.3)**.** Let R be a ring.

1. $\forall n, m \geq 1$, let $a_1, \ldots, a_n \in R$ and $b_1, \ldots, b_m \in R$. Then $\left(\sum_{i=1}^n a_i\right) \cdot \left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$.
2. $\forall a \in R$, $a * 0 = 0 = 0 * a$.
3. $\forall a, b \in R$, $a(-b) = -a(b) = -ab$, where $-b, -a$ are the additive inverses of b, a respectively. In particular, $(-a)(-b) = ab$.

Important Example: Polynomial Rings

Let R be a commutative ring. Then

$$R[x] := \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n | \forall n \geq 0\ a_i \in R\} = \text{"}R \text{ adjoin } x\text{"}.$$

Let $f, g \in R[x]$. Write $f = \sum_{i=0}^n a_i x^i$, $g = \sum_{j=0}^m b_j x^j$. WLOG, assume $m \leq n$. Define $b_{m+1} = b_{m+2} = \cdots = b_n = 0 \in R$, then $f + g := \sum_{i=0}^n (a_i + b_i) x^i$. Also, $fg := \sum_{k=0}^{m+n} c_k x^k$, where $c_k := \sum_{l=0}^k a_l b_{k-l}$.

Lecture 27

Additive Identity: $0 := \sum_i a_i x^i$, $a_i = o \in R\ \forall i \geq 0$.

Multiplicative Identity: $1 := \sum_i a_i x^i$, $a_o = 1 \in R$, $a_i = 0 \in R\ \forall i \geq 1$.

Proposition (27.1)**.** R commutative implies $R[x]$ is commutative.

Remark. $R[x][y]$. This is just a polynomial in 2 variables.

Definition (27.2)**.** Let $f = \sum a_k x^k \in R[x]$, where $\sum a_k x^k$. Then the **degree** of f, $\deg(f) \in \mathbb{N}$ is the largest $n \in \mathbb{Z}$ such that $a_n \neq 0$. Often, $\deg(0) := -\infty$.

Basic Constructions

Definition (27.3)**.** Let R be a ring. A subset $S \subseteq R$ is a **subring** iff

1. $(S, +, 0_R) \leq (R, +, 0_R)$ is a subgroup with respect to $+$.
2. $\forall x, y \in S$, $x * y \in S$. i.e. S is closed under multiplication.
3. $1_R \in S$.

We write $S \leq R$ to denote that S is a subring of R.

Example. 1. We have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

2. Let R be commutative. Then $R \leq R[x]$.

3. (Non-Commutative Examples): Let $R = M_2(\mathbb{R})$ and $S = \left\{A \in R | A = \alpha = \begin{pmatrix} a_1 & a_2 \\ 0 & 3 \end{pmatrix}\right\}$. Then $S \leq R$.

CAUTION!!! Some authors...

1. don't require a ring to have 1 (multiplicative identity)
2. don't require subrings to have $1_R \in S$ (no Axiom 3).

Basic Constructions

1. $n\mathbb{Z} \not\leq \mathbb{Z}$, $n > 1$ since $1 \notin \mathbb{Z}$.
2. If $R \neq \{0_R\}$, then $\{0_R\} \not\leq R$ since $1_R \notin \{0_R\}$.
3. Take $S = \{f = \sum a_i x^2 \in R[x] | a_0 = 0\} \not\leq R[x]$ since $1 \notin R[x]$.

Lecture 28

Ring Homomorphisms

Definition (28.1)**.** Let R, S be rings. A **ring homomorphism** from R to S is a function $\varphi : R \to S$ such that $\forall a,b \in R$,

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$, and
3. $\varphi(1_R) = 1_S$. A **ring isomorphism** is a ring homomorphism φ such that φ is a bijection.

Example. 1. $\mathrm{id} : R \to R$ is a ring isomorphism. BOOOORING!!!

2. Let $n > 1$. Then $\pi : \mathbb{Z} \to \mathbb{Z}/n$, $\pi(a) := [a]$ is a ring homomorphism.
3. (NON-EXAMPLE) Let $\det : M_2(\mathbb{R}) \to \mathbb{R}$ be a function. Then Axioms 2 and 3 are satisfied, but not Axiom 1 since $\det(A+B) \neq \det(A) + \det(B)$ in general.

Proposition (28.2)**.** Let $r \in R$. The function $\mathrm{ev}_r(f) := f(r)$ is a ring homomorphism ("evaluation at r").

In general, elements of $R[x]$ "aren't functions."

Example. $\mathbb{Z}/2[x]$.

$$\deg(-\infty) : \overline{0} \qquad \deg(1) : x, x+\overline{1}$$
$$\deg(0) : \overline{1} \qquad \deg(2) : x^2, x^2+x, x^2+\overline{1}, x^2+x+\overline{1}.$$

The number of ev homomorphisms is 2: $\mathrm{ev}_{\overline{0}}, \mathrm{ev}_{\overline{1}} : \mathbb{Z}/2[x] \to \mathbb{Z}/2$.

Let $f := x^2 + x + \overline{1}$, $g := \overline{1}$. Then $\mathrm{ev}_{\overline{0}}(f) = \overline{1}$, $\mathrm{ev}_{\overline{1}}(f) = \overline{1}^2 + \overline{1} + \overline{1} = \overline{1}$.
Also, $\mathrm{ev}_{\overline{0}}(g) = \overline{1}$, $\mathrm{ev}_{\overline{1}}(g) = \overline{1}$, BUT $f \neq g$.

Definition (28.3)**.** Let $\varphi : R \to S$ be a ring homomorphism. The **kernel** of φ is the subset $\ker(\varphi) := \{r \in R | \varphi(r) = 0_S\}$ of R.
The **image** of φ is the subset $\mathrm{im}(\varphi) := \{\varphi(r) | r \in R\}$ of S.

Proposition (28.4)**.** 1. $\mathrm{im}(\varphi) \leq S$ is a subgroup of S.

2. $\ker(\varphi) \leq R$ is a subring of R iff $S = \{0_S\}$ is the trivial ring.

Lecture 29

Prop 28.4.

1. Want to show $1_S \in \text{im}\varphi$. By definition of φ, $\varphi(1_R) = 1_S$ which implies $1_S \in \text{im}\varphi$. (The rest of this proof is similar to the proof of Proposition 16.1 for groups.

2. ($\implies$) Suppose $\ker\varphi$ is a subring. By definition of subring, $1_R \in \ker\varphi$. Therefore $\varphi(1_R) = 0_S$. On the other hand, $\varphi(1_R) = 1_S$ by definition of ring homomorphism. Let $s \in S$. Then $s = s \cdot 1_S = s \cdot \varphi(1_R) = s \cdot 0_S$. Thus by Proposition 26.3, $s = 0_s$ and therefore $S = \{0_S\}$.
   ($\impliedby$) Suppose $S = \{0_S\}$. Then $\forall r \in R$, $\varphi(r) = 0_S$. Therefore $\ker\varphi = R$. Every ring is a subring of itself.

■

Definition (29.1). Let R be a ring. A subset $I \subseteq R$ is an **ideal** iff

1. I is an additive subgroup of R, i.e. $(I, +, 0_R) \le (R, +, 0_R)$ and
2. $\forall a \in I$ and $\forall r \in R$, $ra \in I$ and $ar \in I$.

We write $I \trianglelefteq R$.

Examples

1. Let R be a ring. Then $0 = \{0_R\}$ and R are both ideals of R.
2. Let $n \ge 1$. Then $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is an ideal.
3. Let $R = \mathbb{R}[x]$, let $g \in \mathbb{R}[x]$, and let $I := \{f \in \mathbb{R}[x] : g|f \text{ i.e. } \exists h \in \mathbb{R}[x] \text{ such that } f = gh\}$. Then $I \trianglelefteq \mathbb{R}[x]$.

Lecture 30

Non-Examples of Ideals

1. None of $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
2. Let R be commutative. Then $R \le R[x]$ is not an ideal (Axiom 2 does not hold).
3. Let $R = \mathbb{Z}$, $C = 2\mathbb{Z} \cup 3\mathbb{Z}$. In this case, Axiom 2 holds, but Axiom 1 fails since $3(1) + 2(-1) = 1 \notin C$.

Proposition (30.1). Let R be commutative, $I, J \trianglelefteq R$ be ideals.

1. $I \cup J$ is not, in general, an ideal of R. However, $I \cap J \trianglelefteq R$.
2. The subset $I + J := \{a + b \in R | a \in I, b \in J\}$ is an ideal of R.
3. The subset $IJ := \{a_1 b_1 + a_2 b_2 + \cdots + a_n b_n | n \in \mathbb{N}, a_i \in I, b_i \in J\}$ is an ideal of R.

Kernels Revisited

Proposition (30.2). Let $\varphi : R \to S$ be a ring homomorphism. Then…

1. $\ker\varphi \trianglelefteq R$
2. $\ker\varphi = 0$ iff φ is injective.

Proof.

1. Since $\varphi(a + b) = \varphi(a) + \varphi(b)\ \forall a, b \in R$, φ is an additive group homomorphism. Therefore $\ker\varphi$ is an additive subgroup of $(R, +, 0_R)$ by Proposition 16.2.
2. This follows directly from Proposition 17.1.

■

Quotient Rings

Let $I \trianglelefteq R$ be an ideal. Forgot about multiplication for a moment. We know $(I, +) \le (R, +)$ is a subgroup.
Let $r \in R$. The left cosets of I are of the form $r + I := \{r + a | a \in I\}$. Recall that $R/I := \{r + I|r]inR\}$ is the set of left cosets. This is a group with respect to addition since $(R.+)$ is abelian.

Lecture 31

Generalize Construction of Z/nZ as a Ring

Theorem (31.1 **PROVE ON EXAM!**)**.**

1. The binary operation $\bar{*} : R/I \times R/I \to R/I$, $(r_1 + I)\bar{*}(r_2 + I) := r_1 r_2 + I$ is well-defined.
2. $(R/I, \bar{+}, 0_{R/I}, \bar{*}, 1_{R/I})$ is a ring, where $1_{R/I} := 1_R + I$.
3. The surjective function $\pi : R \to R/I$, $\pi(r) := r + I$ is a ring homomorphism.

Proof.

1. Suppose $r_1+I = r_1'+I$ and $r_2+I = r_2'+I$ (1). Want to show $r_1r_2+I = r_1'r_2'+I$. Since $r_1 \in r_1+I$, $r_2 \in r_2+I$, (1) implies $\exists a_1, a_2 \in I$ such that $r_1 = r_1'+a_1$, $r_2 = r_2'+a_2$. Therefore $r_1r_2 = (r_1'+a_1)(r_2'+a_2) = r_1'r_2'+r_1'a_2+a_1r_2'+a_1a_2$. By Axiom 2 of Definition 29.1 of ideal, $r_1'a_2$, a_1r_2', $a_1a_2 \in I$. Axiom 1 implies $r_1r_2 - r_1'r_2' \in I$. Therefore by PS5 #1, $r_1r_2 + I = r_1'r_2' + I$.
2. Straightforward. Skip because this is L O N G.
3. Check the axioms of ring homomorphism:
   (a) $\pi(r_1 + r_2) = (r_1 + r_2) + I = (r_1 + I)\bar{+}(r_2 + I) = \pi(r_1)\bar{+}\pi(r_2)$.
   (b) $\pi(r_1 r_2) = r_1 r_2 + I = (r_1 + I)\bar{*}(r_2 + I) = \pi(r_1)\bar{*}\pi(r_2)$.
   (c) $\pi(1_R) = 1_R + I = 1_{R/I}$.

■

Example (Non-Example)**.** (Replace ideal with a subring in R/I). Consider: $\mathbb{Z} \le \mathbb{Q}$ and the quotient group $\mathbb{Q}/\mathbb{Z}$ $(q_1+\mathbb{Z})\bar{+}(q_2+\mathbb{Z}) = (q_1+q_2)+\mathbb{Z}$. Then $(\frac{1}{2}+\mathbb{Z})\bar{+}(\frac{1}{3}+\mathbb{Z}) = \frac{1}{6}+\mathbb{Z}$. Note that $\frac{1}{2}+\mathbb{Z} = \frac{3}{2}+\mathbb{Z}$. Then $(\frac{3}{2}+\mathbb{Z})\bar{+}(\frac{1}{3}+\mathbb{Z}) = \frac{1}{2}+\mathbb{Z} \neq \frac{1}{6}+\mathbb{Z}$.

1st Isomorphism Theorem for Rings

Theorem (31.2)**.** let $\varphi : R \to S$ be a ring homomorphism. Then the function $\overline{\varphi} : R/\ker\varphi \to \mathrm{im}\varphi$, $\overline{\varphi}(r+\ker\varphi) := \varphi(r)$ is a well-defined ring isomorphism.

Lecture 32

Properties of Elements in Rings

Recall from Lecture 6 the following:

Theorem (6.2)**.** $(\mathbb{Z}/n^{\times}, *, [0])$, where $\mathbb{Z}/n^{\times} := \{[k] \in \mathbb{Z}/n - \{[0]\} | \gcd(k,n) = 1\}$ for $n > 1$ is a group.

Example. We have $Z/4^{\times} = \{[1],[3]\}$. Here, $[1] * [1] = [1]$ and $[3] * [3] = [8] = [1]$. Therefore, every element has a multiplicative inverse. Also, if you have $[a],[b] \in \mathbb{Z}/4$ such that $[a] * [b] = [0]$, then $[a],[b]$ need not be $[0]$: $[2]*[2] = [4] = [0]$. On the other hand, if $n = p$ prime, then $(\mathbb{Z}/p^{\times}) = \mathbb{Z}/p - \{[0]\}$. Every non-zero element of $\mathbb{Z}/p$ has a multiplicative inverse.

Definition (32.1)**.** Let R be a ring. An element $a \in R$ is a **unit** iff it has a multiplicative inverse. i.e. $\exists u \in R$ such that $au = ua = 1_R$. Define $R^{\times} := \{a \in R | a \text{ is a unit}\}$.

Proposition (32.2)**.** Let $(R, +, 0_R, *, 1_R)$ be a ring. Then...

1. $(R^{\times}, *, 1_R)$ is a group.
2. If $a \in R^{\times}$, its inverse is unique.
3. If $1_R \neq 0_R$, $0_R \notin R^{\times}$.

Proof.

1. Definition of a ring implies $(R, *, 1_R)$ is a monoid. This implies $*$ is associative and 1_R is the identity element. Now we need to show $R^{\times}$ is closed with respect to $*$. Let $a, b \in R^{\times}$, and let u, w be the inverses, respectively. WTS $a * b \in R^{\times}$. We have $a * u = 1_R = u * a$ and $b * w = 1_R = w * a$. Now consider $(w * u) * (a * b) = w*(u*a)*b = w*1_R*b = w*b = 1_R$. So $(a*b)*(w*u) = a*(b*w)*u = a*1_R*u = a*u = 1_R$. Therefore $a*b \in R^{\times}$.

2. By 1. above, $R^\times$ is a group which implies that the inverse of any element in the group is unique.

3. Use the contrapositive. Suppose $0_R \in R^\times$. By definition, $\exists u \in R$ such that $0_R u = 1_R$. Thus, $0_R u = 0_R$ by 26.3.

■

Definition (32.3)**.** A ring R is a **division ring** iff $R^\times = R - \{0_R\}$. A **field** is a commutative division ring. Fields are denoted $\mathbb{K}$.

Examples of fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p := \mathbb{Z}/p$.

Another example: $\mathbb{K}(x) := \left\{ \frac{p(x)}{q(x)} \middle| p, q \in \mathbb{K}[x],\ q \neq 0 \right\}$. These are rational functions in 1 variable.

Lecture 33

Example (A division ring, but not a field)**.** The quarternions: $\mathbb{H} := \{a + ib + jc + kd | a, b, c, d \in \mathbb{R}\}$, where $i * i = j * j = k * k = -1 \in \mathbb{R}$, $i * j = k$, $j * i = -k$ (non-commutative). If $q = a + ib + jc + kd$, then $\overline{q} := a - ib - jc - kd$ is the conjugate of q and $q * \overline{q} = a^2 + b^2 + c^2 + d^2$.
For $q \neq 0 \in \mathbb{H}$, $q^{-1}q = qq^{-1} = 1$, $q^{-1} = \frac{\overline{q}}{q\overline{q}}$.
Subrings: $\mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$. Group of Units: $\mathbb{R}^\times \leq \mathbb{C}^\times \leq \mathbb{H}^\times$ subgroups. "Norm 1 integer units": $\{\pm 1\} \leq \{\pm 1, \pm i\} \leq \{\pm 1, \pm i, \pm j, \pm k\}$.

Definition (33.1)**.** Let $R \neq 0$ be a ring. An element $a \neq 0 \in R$ is a **zero divisor** if $\exists b \neq 0$ such that $ab = 0$ or $ba = 0$.

Example.

1. $[3] \in \mathbb{Z}/6$ is a zero divisor since $[3] \cdot [2] = [6] = [0]$, but $[3] \neq [0]$, $[2] \neq [0]$.
2. Let R be a non-trivial ring: $R \times R$. Then an element $(1,0) \cdot (0,1) = (0,0)$ is a zero divisor.
3. For the integers $\mathbb{Z}$, there exists no such zero divisor.

Definition (33.2)**.** A ring R is an **integral domain** iff

1. $R \neq 0$
2. R is commutative
3. R has no zero divisors

Proposition (33.3)**.** A field $\mathbb{K}$ is an integral domain.

Remark. An **entire ring** as defined in Paulin's notes is a ring $R \neq 0$ that has no zero divisors.

Polynomial Rings and Zero Divisors

Suppose $f, g \in \mathbb{R}[x] - \{0\}$. Then $\deg(f) = m$, $\deg(g) = n$, and $\deg(fg) = m + n$.
On the other hand, $f = [3]x^3$, $g = [2]x^2 + x \in \mathbb{Z}6[x]$. So $\deg(f) = 3$, $\deg(g) = 2$, and $\deg(fg) = [3]x^4 < \deg(f) + \deg(g)$.

Theorem (33.4)**.** Let R be an integral domain. Then...

1. If $f, g \in R[x] - \{0_R\}$, then $\deg(fg) = \deg(f) + \deg(g)$.
2. $\mathbb{R}[x]$ is an integral domain.

Lecture 34

Proof (Thm 33.4).

1. Let $\deg f = n \geq 0$, $\deg g = m \geq 0$. Then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$ for a_i, $b_j \in R$. By definition of degree, $a_n \neq 0$ and $b_m \neq 0$. Consider $fg = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + a_0 b_0$. Note that $a_n b_m \neq 0$ since R is an integral domain and $a_n \neq 0$, $b_n \neq 0$. So $\deg fg = n + m = \deg f + \deg g$.
2. Let f, $g \in R[x] - \{0\}$. WTS $fg \neq 0$. Therefore $\deg f = n \geq 0$, $\deg g = m \geq 0$. Therefore as in 1. above, we have $fg = a_n b_m x^{n+m} + \cdots$ with $a_n \neq 0$ and $b_m \neq 0$. Thus $a_n b_m x^{n+m} \neq 0$ implies $fg \neq 0$.

■

Corollary (34.1)**.** If $\mathbb{K}$ is a field, then $\mathbb{K}(x)$ is an integral domain.

Remark. If R is an integral domain and we have $ac = bc$ in R with $c \neq 0$, then $a = b$.

Principal and Prime Ideals in Commutative Rings

From here on, R is assumed to be a non-trivial commutative ring (so $0_r \neq 1_r$).

Proposition (34.2)**.** Let $a \in R$. The subset $(a) := \{ra | r \in R\} \subseteq R$ is an ideal called the **principal ideal** generated by a.

Example. We have $n\mathbb{Z} = (n)$ when $R = \mathbb{Z}$.

Definition (34.3)**.** An ideal $I \trianglelefteq R$ is **principal** iff $\exists a \in I$ such that $I = (a)$.

Theorem (34.4)**.** Every ideal in $\mathbb{Z}$ is principal.

Proof. Suppose $I \trianglelefteq \mathbb{Z}$ is an ideal. By definition of ideal, $(I, +, 0) \leq (\mathbb{Z}, +, 0)$ is a subgroup. Recall $\mathbb{Z}$ is a cyclic (additive) group. In particular, $\mathbb{Z} = \langle 1 \rangle$. Theorem 13.3 says every subgroup of a cyclic group is cyclic. Therefore $\exists n \in I$ such that $I = \langle n \rangle = n\mathbb{Z}$. As an ideal, $n\mathbb{Z} = (n)$. ■

Lecture 35

An ideal $I \trianglelefteq R$ is **principal** iff $\exists a \in I$such that $I = (a) = \{ra | r \in R\}$.

Example.

1. Let $R = \mathbb{Z}$, $I = n\mathbb{Z} = (n)$.
2. For every ring, the zero ideal is principal and R is a principal ideal (i.e. $\{0_R\} = (0)$), $R = (1)$.)

Definition (35.1)**.** A ring R is a **principal ideal ring (PIR)** iff every ideal of R is principal.
R is a **principal ideal domain (PID)** iff R is an integral domain and R is a PIR.

Recall Theorem 34.4 which stated that $\mathbb{Z}$ is a PID (wasn't worded like this).

Proposition (35.2)**.** $\forall n > 1$, $\mathbb{Z}/n/Z$ is a PIR.

Proposition (35.3)**.** A field $\mathbb{K}$ has exactly 2 ideals: the zero ideal and $\mathbb{K}$.

Corollary (35.4)**.**

1. A field is a PID.
2. If $\mathbb{K}$ is a field and $\varphi : \mathbb{K} \to S$ is a ring homomorphism, then φ is injective OR S is the zero ring.
3. $\mathbb{Z}/n\mathbb{Z}$ is a PID if n is prime.

Remark (35.5)*.*

1. Nice Theorem in Paulin: "If R is a finite integral domain, then R is a field." So, $\mathbb{Z}/n\mathbb{Z}$ being an integral domain implies $(\mathbb{Z}/n\mathbb{Z})^\times = \{[k] | \gcd(k, n) = 1\} = \{[1], [2], \ldots, [n-1]\}$ since this is a field. Therefore if $d | n$ and $d < n$, then $d = 1$. Thus n is prime and we conclude $\mathbb{Z}/n\mathbb{Z}$ is a PID iff $\mathbb{Z}/n\mathbb{Z}$ is a field iff $n = p$ prime.
2. $\mathbb{Z}[x]$ is an integral domain by Theorem 33.4, but is not a PID.

How to Get More Examples of PIDs?

Recall in Theorem 13.3 (wayyyy back then), we showed that every subgroup of a cyclic group is cyclic. Crucial in our proof was the division algorithm in $\mathbb{Z}$.

Definition (35.6)**.** Let R be a commutative ring such that $0 \neq 1$.

1. A **Euclidean function** on R is a set-theoretic function $N : R - \{0_R\} \to \mathbb{N} \cup \{0\}$ such that
   (a) $\forall a \in R$, $\forall b \in R - \{0_R\}$, $N(a) \leq N(ab)$.
   (b) $\forall a \in R$ and $\forall b \neq 0 \in R$, $\exists q, r \in R$ such that $a = bq + r$ with either $r = 0$ OR $N(r) < N(b)$.
2. An integral domain is the **Euclidean domain** iff R admits a Euclidean function.

Theorem (35.7)**.** The following are Euclidean domains:

1. $\mathbb{Z}$ with $N(m) := |m|$ $\forall m \neq 0$ (absolute value).
2. Any field $\mathbb{K}$ with $N(a) := 1$ $\forall a \neq 0 \in \mathbb{K}$.
3. $\mathbb{Z}[i]$ with $N(k + ib) := a^2 + b^2$ $\forall a + ib \neq 0$.
4. Polynomial Ring $\mathbb{K}[x]$ with coefficients in a field $\mathbb{K}$, $N(f) := \deg(f)$ $\forall f \neq 0$.

Lecture 36

Proposition (36.1)**.** Every ED is a PID.

Example.

Definition (36.2)**.** A deg(n) polynomial is **monic** iff its leading coefficient is 1_R i.e. $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$.

Corollary (36.3)**.** If $\mathbb{K}$ is a field and $I \trianglelefteq \mathbb{K}[x]$ is a non-trivial ideal, then $\exists f \neq 0 \in I$ such that $I = (f)$, f is monic, and $\deg(f) \leq \deg(g)$ $\forall g \in I - \{0\}$.

Primes and Irreducibles

Definition (36.4)**.** 1. An element $a \in R$ **divides** $b \in R$ iff $\exists r\ inR$ such that $b = ra$. Write $a|b$.

2. An element $p \in R$ is **prime** iff
   (a) $p \neq 0$ and p is not a unit (i.e. p has no multiplicative inverse).
   (b) Whenever $p|ab$, then $p|a$ or $p|b$.
3. An element $c \in R$ is **irreducible** iff
   (a) $c \neq 0$ and c is not a unit.
   (b) If $c = ab$, then either a or b is a unit.

Proposition (36.5)**.** If R is an integral domain, then prime is irreducible.

Lecture 37

Example. Claim: Let $q = \pm \in \mathbb{Z}$ with p a prime number. Then

- q is a prime element of $\mathbb{Z}$ and
- q is an irreducible element of Z.

Example. Recall that a non-constant polynomial $f \in \mathbb{K}[x]$ is irreducible if it can't be factored into 2 non-constant polynomials, i.e. if $f = gh$, then $\deg(g) = 0$ or $\deg(h) = 0$.
Fact: Units of $\mathbb{K}[x]$ = non-zero constants = $\mathbb{K}^{\times}$. Hence f an irreducible polynomial implies f is an irreducible element in $\mathbb{K}[x]$.

Example. $\forall a \in \mathbb{K}$, $x - a$ is irreducible in $\mathbb{K}[x]$. Note that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but $x^2 + 1$ is NOT irreducible in $\mathbb{K}[x]$ if $\sqrt{-1} \in \mathbb{K}$.

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Note that $a + b\sqrt{-5}$ is a unit in R iff $a^2 + 5b^2 = 1$. Also, $3 = 3 + 0\sqrt{-5} \in R$ is irreducible. BUT 3 is not prime!! Let $a = 2 + \sqrt{-5}$, $b = 2 - \sqrt{-5} \in R$. Then $ab = 4 + 5 = 9$. Therefore, $3|ab$, but in $\mathbb{Z}[\sqrt{-5}]$, $3 \nmid 2 + \sqrt{-5}$ and $3 \nmid 2 - \sqrt{-5}$. Therefore, irreducible element does not imply prime element.

Example. Claim: Let $n \geq 2 \in \mathbb{N}$ be composite, p be a prime number such that $p|n$. Then $[p] \in \mathbb{Z}/n\mathbb{Z}$ is a prime element.

Lecture 38

Remark. Recall in $\mathbb{Z}$, $q = \pm p$ with p a prime number. Then in q is prime and irreducible $\mathbb{Z}^{\times} = \{\pm 1\}$. Slogan: "Primeness doesn't care about multiplying by units."

Definition (38.1)**.** Let R be a commutative ring not equal to 0.

1. An ideal $P \trianglelefteq R$ is **prime ideal** iff for $P \neq R$ whenever, $ab \in P$, then either $a \in P$ or $b \in P$.
2. An ideal $M \trianglelefteq R$ is **maximal** iff $M \neq R$ and whenever $J \trianglelefteq R$ is an ideal with $M \subseteq J$, then either $J = R$ or $J = M$.

Example (38.2)**.** $\mathbb{K}$ is a field, $f \in \mathbb{K}[x]$ irreducible polynomial (e.g. $f = x - 1$). Claim: $(f) \trianglelefteq \mathbb{K}[x]$ is maximal.

1. Note $1 \notin (f)$ since $\deg 1 = 0$ and $\deg f \geq 1$.
2. Suppose $J \trianglelefteq \mathbb{K}[x]$ such that $(f) \subseteq J$. Proposition 36.1 implies $\exists g \in J$ such that $J = (g)$. $(f) \subseteq J$ implies $f \in (g)$. Therefore $\exists h \in \mathbb{K}[x]$ such that $f = gh$. f irreducible implies either g or h is a non-zero constant.
   (a) If g is a unit, then $J = (g) = (1) = \mathbb{K}[x]$.
   (b) If h is a unit, then $\exists h^{-1} \in \mathbb{K}^{\times}$ such that $h^{-1}h = 1$ which implies $g = h^{-1}f$. Therefore $J = (g) = (h^{-1}f) = (f)$.

Theorem (38.3)**.** Let R be a commutative non-trivial ring, and $I \trianglelefteq R$ be an ideal. Then

1. I is a prime ideal iff R/I is an integral domain.
2. I is maximal ideal iff R/I is a field.

Remark (38.4). Since every field is an integral domain, Theorem 38.3 implies every maximal ideal is a prime ideal.

Theorem (38.5)**.** Let R be a PID. Then $p \in R$ is prime iff p is irreducible.