Groups, Rings, and Modules

Jonathan Gai

March 2, 2022

Contents

Lecture 1: Groups

20 Jan. 12:00

Introduction

Groups

Continuation from IA, focussing on

1. Simple groups, p-groups, p-subgroups.
2. Main results in this part of the course will be the Sylow Theorems.

Rings

Sets where you can add, subtract and multiply.

Example. Examples of rings include,

1. $\mathbb{Z}$ or $\mathbb{C}[X]$.
2. Rings of integers $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ (More in Part II Number Fields).
3. Polynomial rings $\mathbb{C}[x_1, \ldots, x_2]$ (More in Part II Algebraic Geometry).

A ring where you can divide is called a *field*.

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Modules

An analogue of vector space where the scalars belong to a ring instead of a field.

We will classify modules over certain nice rings.

Allows us to prove Jordan normal form, and classify finite Abelian groups.

1 Groups

1.1 Revision and Basic Theory

We revisit basic properties and definition from Part IA Groups.

Definition 1.1 (Group). A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

1. (Associativity) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. (Identity) $\exists a \in G$ s.t. $e \cdot g = g \cdot e = g \ \forall g \in G$.
3. (Inverses) $\forall g \in G, \exists y^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Remark. Some things to note form definition of a group.

1. *Closure* is included implicitly in the definition of a binary operation. In checking $\cdot$ well-defined, we need to check closure, i.e. $a, b \in G \implies a \cdot b \in G$.
2. If using additive (or multiplicative) notation, often write 0 (or 1) for identity.

Definition 1.2 (Subgroup). A subset $H \subset G$ is a *subgroup* (written $H \leq G$) if $h \cdot h^{-1} \in H, \forall h, h' \in H$, and $(H, \cdot)$ is a group. Remark: A non-empty subset H of G is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$

Example. Here we list some common groups and their subgroups.

1. Additive $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
2. Cyclic and dihedral group, $C_n \leq D_{2n}$.
3. Abelian groups - those $(G, \cdot)$ such that $a \cdot b = b \cdot a \ \forall a, b \in G$
4. Symmetric and Alternating groups, $A_n \leq S_n$.
5. Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.
6. General and Special Linear Groups, $SL_n(\mathbb{R}) \leq SL_n(\mathbb{R})$.

Definition 1.3 (Direct Product). The *(direct) product* of groups G and H is the set $G \times H$ with operation given by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Let $H \leq G$, the *left cosets* of H in G are the sets $gH = \{gh \mid h \in H\}$ for $g \in G$. These partition G, and each coset has the same cardinality as H. So we can deduce.

Theorem 1.1 (Lagrange's Theorem). Let G be a finite group and $H \leq G$, Then $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the number of left cosets of H in G. $[G : H]$ is the *index* of H in G.

Remark. Can also carry this out with right cosets. Lagrange's Theorem then implies that the number of left cosets is the same as the number of right cosets.

Definition 1.4 (Order). Let $g \in G$. If $\exists n \geq 1$ s.t. $g^n = 1$ then the least such n is the *order* of g, otherwise we say that g has infinite order.

Remark. If g has order d, then

1. $g^n = 1 \implies d \mid n$.
2. $\{1, g, \ldots, g^{d-1}\} \leq G$ and so if G is finite, then $d \mid |G|$ (by Lagrange's Theorem).

Definition 1.5 (Normal Subgroup). A subgroup $H \leq G$ is *normal* if $g^{-1}Hg = H \ \forall g \in G$. We write $H \trianglelefteq G$.

Proposition 1.1. If $H \trianglelefteq G$ then the set G/H of left cosets of H in G is a group (called the *quotient group*) with operation

$$g_1 H \cdot g_2 H = g_1 g_2 H.$$

Proof. Check that $\cdot$ is well-defined.

Suppose $g_1 H = g_1' H$ and $g_2 H = g_2'$. Then $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$, we have

$$\begin{aligned} g_1' g_2' &= g_2 h_1 g_2 h_2 \\ &= g_1 g_2 (g_2^{-1} h_2 g_2) h_2 \end{aligned}$$

so $g_1' g_2' H = g_1 g_2 H$.

Associativity is inherited from G, the identity is $H = eH$, and the inverse of gH is $g^{-1}H$. ∎

Definition 1.6 (Homomorphism). G, H groups. A function $\phi : G \to H$ is a group homomorphism if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \forall g_1, g_2 \in G$. It has *kernel*

$$\ker(\phi) = \{y \in G \mid \phi(y) = 1\} \trianglelefteq G,$$

and *image* $\mathrm{Im}(\phi) = \{\phi(y) \mid y \in G\} \leq H$.

Proof. If $a \in \ker(\phi)$ and $g \in G$, then

$$\begin{aligned}\phi(g^{-1}ag) &= \phi(g^{-1})\phi(a)\phi(g) \\ &= \phi(g^{-1})\phi(g) \\ &= \phi(g^{-1}g) \\ &= \phi(1) \\ &= 1.\end{aligned}$$

So it is indeed a normal subgroup. ∎

Lecture 2: Isomorphism Theorems

22 Jan. 12:00

We will next talk about a special kind of homomorphism.

Definition 1.7. An *isomorphism* of groups is a group homomorphism that is also a bijection.

We say that G and H are isomorphic (written $G \cong H$) if there exists an isomorphism $\phi : G \to H$.

Exercise. Check that $\phi^{-1} : H \to G$ is a group homomorphism.

Theorem 1.2 (First Isomorphism Theorem). Let $\phi : G \to H$ be a group homomorphism. Then $\ker(\phi) \trianglelefteq$ and $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Proof. Let $K = \ker(\phi)$. We already checked that K is normal.

Define $\Phi : G/K \to \mathrm{Im}(\phi)$, $gK \mapsto \phi(g)$. We need to check that Φ is well-defined first.

$$\begin{aligned}g_1K = g_2K &\iff g_2^{-1}g_1 \in K \\ &\iff \phi(g_2^{-1}g_1) = 1 \\ &\iff \phi(g_1) = \phi(g_2).\end{aligned}$$

Note that we showed that Φ is injective at the same time because we can just go the other way.

Next, we show that Φ is a group homomorphism.

$$\begin{aligned}\Phi(g_1Kg_2K) &= \Phi(g_1g_2K) \\ &= \phi(g_1g_2) \\ &= \Phi(g_1K)\Phi(g_2K).\end{aligned}$$

Lastly, we show that Φ is surjective. Let $x \in \mathrm{Im}(\phi)$, say $x = \phi(g)$ for some $g \in G$, then $x = \Phi(gK)$. So it is indeed an isomorphism. ■

Example. If we consider the function

$$\begin{aligned} \phi\colon \mathbb{C} &\longrightarrow \mathbb{C}^\times \\ z &\longmapsto e^z \end{aligned}$$

Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +) \to (\mathbb{C}, \times)$. It is well known that

$$\begin{aligned} \ker(\phi) &= 2\pi i\mathbb{Z}, \\ \mathrm{Im}(\phi) &= \mathbb{C}^\times \quad \text{by existence of log .} \end{aligned}$$

Thus, $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^\times$.

From the naming for the First Isomorphism Theorem, we have the following Isomorphism Theorems as well.

Theorem 1.3 (Second Isomorphsim Theorem). Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk \mid h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Proof. Let $h_1k_1, h_2k_2 \in HK$ with $h_1, h_2 \in H$, $g_1, g_2 \in G$. It suffices to show that

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1h_2^{-1}}_{H}\underbrace{(h_2k_1k_2^{-1}h_2^{-1})}_{K} \in HK.$$

Thus, $HK \leq G$ by remark from last lecture. Let

$$\begin{aligned} \phi\colon H &\longrightarrow {}^{G}/_{K} \\ h &\longmapsto hK. \end{aligned}$$

This is the composition of inclusion map $H \to G$ and quotient map $G \to {}^{G}/_{K}$ hence ϕ is a group homomorphism.

$$\begin{aligned} \ker(\phi) &= \{h \in H \mid hK = K\} = H \cap K \trianglelefteq H, \\ \mathrm{Im}(\phi) &= \{hK \mid h \in H\} = {}^{HK}/_{K}. \end{aligned}$$

First isomorphism theorem gives

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

■

Remark. Suppose $K \trianglelefteq G$, there is a bijection

$$\begin{aligned} \{\text{Subgroups of } {}^{G}/_{K}\} &\longleftrightarrow \{\text{Subgroups of } G \text{ containing } K\}, \\ x &\longmapsto \{g \in G \mid gK \in X\}, \\ {}^{H}/_{K} &\longleftarrow\!\shortmid H. \end{aligned}$$

Restricts to a bijection between the normal subgroups.

$$\{\text{Normal subgroups of } {}^{G}/_{K}\} \longleftrightarrow \{\text{Normal subgroups of } G \text{ containing } K\}.$$

Theorem 1.4 (Third Isomorphism Theorem). Let $K \leq H \leq G$ be normal subgroups of G. Then

$$\frac{{}^{G}/_{K}}{{}^{H}/_{K}} \cong \frac{G}{H}.$$

Proof. Let

$$\begin{aligned} \phi\colon {}^{G}/_{K} &\longrightarrow {}^{G}/_{H} \\ gK &\longmapsto gH. \end{aligned}$$

If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K \leq H \implies g_1H = g_2H$. So ϕ is well-defined.

ϕ is a surjective group homomorphism with $\ker(\phi) = {}^{H}/_{K}$.

Now apply First Isomorphism Theorem. ■

If $K \trianglelefteq G$, then studying the group K and ${}^{G}/_{K}$ gives some information about G.

This approach is not always available.

Definition 1.8 (Simple Group). A group G is *simple* if $\mathbf{1}$ (the trivial subgroup) and G are its only normal subgroups.

Notation. We do not consider the trivial group to be a simple group.

Similar to the prime numbers, we can think of finite simple groups as the building block of finite groups. One of the greatest achievements in math is that we classified *all* finite simple groups!

Lemma 1.1. Let G be an Abelian group. G is simple if and only if $G \cong C_p$ for some prime p.

Proof. We prove the $\impliedby$ direction first. Let $H \leq C_p$. Lagrange's Theorem tells us

$$|H||C_p| = p.$$

So $|H| = 1$ or p by primality of p. That is, $H = \{1\}$ or C_p. Thus, C_p is simple.

To prove the $\implies$ direction. Let $1 \neq g \in G$. G contains the subgroup

$$\langle g \rangle = \langle \ldots, g^{-2}, g^{-1}, e, g, g, \ldots \rangle$$

which is the subgroup generated by g. It is normal in G since G is Abelian. Since G simple, $\langle g \rangle = G$.

If G is infinite, $G \cong (\mathbb{Z}, +)$ which cannot be true by simplicity of G because $2\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Otherwise, $G \cong C_n$ for some n, let g be a generator. If $m \mid n$, then $g^{n/m}$ generates a subgroup of order m. Because G is simple, the order of the subgroup can only be 1 or n. So the only factors of n is 1 and n, and we have n prime. ■

Lemma 1.2. If G is a finite group, then it has a composition series

$$\mathbf{1} \cong G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m \cong G$$

with each quotient G_{i+1}/G_i simple.

Note that G_i need not be normal in G.

Lecture 3

25 Jan. 1:00

Proof. Induct on $|G|$. When $|G| = 1$, the statement is obviously true.

If $|G| > 1$, let G_{m-1} be a normal subgroup of the largest possible order that is not $|G|$. By the correspondence theorem, G/G_{m-1} is simple.

Apply inductively to G_{m-1}. ■

1.2 Group Action

Definition 1.9. For X a set, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition. The identity is $id = id_X$.

A group G is a *permutation group* of degree n if $G \leq$ X with $|Z| = n$.

Example.

1. $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n, as is $A_n \leq S_n$.
2. D_{2n}, the symmetries of regular n-gon, is a subgroup of $\mathrm{Sym}(n)$.

Definition 1.10. An *action* of a group G on a set X is a function $* : G \times X \to X$ satisfying

1. $e * x = x$ for all $x \in X$,
2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G, x \in X$.

Proposition 1.2. An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. For each $g \in G$ let $\phi_g : X \to X$, $x \mapsto g * x$. We have

$$\begin{aligned}\phi_{g_1 g_2}(x) &= (g_1 g_2) * x \\ &= g_1 * (g_2 * x) \\ &= \phi_{g_1}(g_2 * x) \\ &= \phi_{g_1} \circ \phi_{g_2}(x).\end{aligned}$$

Thus, $\phi_{g_1 g_2} = \phi_{g_1}\phi_{g_2}$.

In particular $\phi_{g_1} \circ \phi_{g_1^{-1}} = \phi_{g_1^{-1}} \circ \phi_{g_1} = \phi_e = id_X$.

Because ϕ_g has an inverse, it is bijective. So $\phi_g \in \mathrm{Sym}(X)$. Define

$$\begin{aligned}\phi\colon G &\longrightarrow \mathrm{Sym}(X) \\ g &\longmapsto \phi_g\end{aligned}$$

which is indeed a group homomorphism.

Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a gruop homomorphism.

Define

$$\begin{aligned}*\colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto \phi(g)(x).\end{aligned}$$

Then it does satisfy the requirements for a group action,

1. $e * x = \phi(e)(x) = id_X(x) = x$,
2. $$\begin{aligned}(g_1 g_2) * x &= \phi(g_1 g_2)(x) \\ &= \phi(g_1)(\phi(g_2)(x)) \\ &= g_1 * (g_2 * x).\end{aligned}$$

■

Definition 1.11. We say $\phi : G \to \mathrm{Sym}(X)$ is a *permutation representation* of G.

Definition 1.12. Let G act on a set X.

1. The *orbit* of $x \in X$ is $\mathrm{orb}_G(x) = \{g * x \mid g \in G\} \subseteq X$
2. the *stabilizer* of $x \in X$ is $G_x = \{g \in G \mid g * x = x\} \leq G$.

Recalled from IA, we have the Orbit-Stabilizer Theorem. There is a bijection $\mathrm{orb}_G(x) \leftrightarrow {}^{G}/_{G_x}$, the set of left cosets in G.

In particular, if G is finite, then

$$|G| = |\mathrm{orb}_G(x)||G_x|.$$

Example. Let G be the group of all symmetries of a cube, and X be the set of vertices. Let $x \in X$ be any vertex $|\mathrm{orb}_G(x)| = 8, |G_x| = 8$. So $|G| = 48$.

Remark. 1. $\ker\phi = \cap_{x\in X} G_x$ is called the *kernel* of the group action.

2. The orbits partition X. We say that the action is *transitive* if there is just one orbit.

3. $G_{g*x} = gG_xg^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilizers are conjugate.

Example.

1. Let G act on itself by left multiplication. That is, $g * x = gx$. The kernel of this action is
$$\{g \in G \mid g * x = x \ \forall x \in G\} = \mathbf{1}.$$
Thus, G injects into $\mathrm{Sym}(G)$. This proves,

Theorem 1.5 (Cayley's Theorem). Any finite group G is isomorphic to a subgroup of S_n for some n (take $n = |G|$).

2. Let $H \leq G$, G acts on G/H, the set of left cosets, by left multiplication. That is $g * xH = gxH$.

This action is transitive (since $(x_2x_1^{-1})x_1H = x_2H$) with
$$\begin{aligned} G_{xH} &= \{g \in G \mid gxH = xH\} \\ &= \{g \in G \mid x^{-1}gx \in H\} \\ &= xHx^{-1}. \end{aligned}$$
Thus, $\ker(\phi) = \cap_{x\in G} xHx^{-1}$. This is the largest normal subgroup of G that is contained in H

Theorem 1.6. Let G be a non-Abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq 5$ and G is isomorphic to a subgroup of A_n.

Proof. Let G act on $X = G/H$ by left coset multiplication, and let $\phi : G \to \mathrm{Sym}(X)$ be associated permutation representation.

As G is simple, $\ker(\phi) = \mathbf{1}$ or G. Since G acts transitively on X and $|X| > 1$, $\ker(\phi) = \mathbf{1}$ and $G \cong \mathrm{Im}(\phi) \leq S_n$.

Since $G \leq S_n$ and A_n is a normal subgroup of S_n. The Second Isomorphism Theorem gives $G \cap A_n \cong GA_n/A_n \leq S_n/A_n \cong C_2$. Because G is simple, we have $G \cap A_n = 1$ or G. If the intersection is trivial, we have an injection into C_2 by First Isomorphism Theorem, but G is non-Abelian. So we must have
$$G \cap A_n = G \implies G \leq A_n.$$
Finally, if $n \leq 4$, it is easy to check that A_n does not have non-Abelian simple subgroups. So we must have $n > 5$. ∎

Lecture 4

27 Jan. 12:00

3. If G is a group. Let G act on itself by conjugation. That is $g * x = gxg^{-1}$. We have the following definitions.

$$\begin{aligned} \mathrm{orb}_G(x) &= \{gxg^{-1} \mid g \in G\} = \mathrm{ccl}_G(x) && \textit{(conjugacy class)} \\ G_x &= \{g \in G \mid gx = xg\} = C_G(x) \leq G && \textit{(centralizer)} \\ \ker(\phi) &= \{g \in G \mid gx = xg \ \forall x \in G\} = Z(G) \leq G. && \textit{(center)} \end{aligned}$$

Note. The map $\phi(g) : G \to G$ satisfies $h \mapsto ghg^{-1}$ is a group homomorphism, and also a bijection. That is, it is an isomorphism from G to itself.

Definition 1.13. $\mathrm{Aut}(G) = \{\text{isomorphisms } f : G \to G\}$.

Then $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$, and $\phi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G)$.

4. Let X be set of all subgroups of G, then G acts on X by conjugation. That is, $g * H = gHg^{-1}$.

   The stabilizer of H is $\{g \in G \mid gHg^{-1} = H = N_G(H)\}$, called the *normalizer* of H in G. This is the largest subgroup of G containing H as a normal subgroup.

   In particular $H \trianglelefteq G \iff N_G(H) = G$.

1.3 Alternating Groups

In Part IA, we showed that the elements in S_n are conjugate if and only if they have the same cycle type.

Example. In S_5, we have the following table.

Cycle type	Number of Elements	Sign
1	1	+
(* *)	10	-
(* *)(* *)	15	+
(* * *)	20	+
(* *)(* * *)	20	-
(* * * *)	30	-
(* * * * *)	24	+
Total	120	

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. If there is an odd permutation commuting with g,

$$|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)| \text{ and } |\mathrm{ccl}_{A_n}(g)| = |\mathrm{ccl}_{S_n}(g)|.$$

Otherwise,

$$|C_{A_n}(g)| = |C_{S_n}(g)| \text{ and } |\mathrm{ccl}_{A_n}(g)| = \frac{1}{2}|\mathrm{ccl}_{S_n}(g)|.$$

Example. When $n = 5$, (1 2)(3 4) commutes with (1 2), and (1 2 3) commutes with (4 5). But if $h \in C_{S_5}(g)$, $g = (1\ 2\ 3\ 4\ 5)$, then

$$\begin{aligned}(1\ 2\ 3\ 4\ 5) &= h(1\ 2\ 3\ 4\ 5)h^{-1} \\ &= (h(1)\ h(2)\ h(3)\ h(4)\ h(5)),\end{aligned}$$

so $h \in \langle g \rangle \leq A_5$, and it does split. Thus, A_5 has conjugacy classes of sizes $1, 15, 20, 12, 12$.

To show the simplicity of A_5. If $H \trianglelefteq A_5$, then H is a union of conjugacy classes,

$$\implies |H| = 1 + 15a + 20b + 12c$$

with $a, b \in \{0, 1\}$ and $c \in \{0, 1, 2\}$, and by Lagrange's Theorem $|H| \mid 60$. So by simple arithmetic, $|H| = 1$ or 60. That is A_5 is simple.

Lemma 1.3. A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions. Thus suffices to write the product of any two transpositions as a product of 3-cycles.

We have

- $(a\ b)(b\ c) = (a\ b\ c)$,
- $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$.

■

Lemma 1.4. If $n \geq 5$, then all 3-cycles in A_n are conjugate.

Proof. We claim that every 3-cycle is conjugate to 1 2 3. Indeed, if $(a\ b\ c) = \sigma(1\ 2\ 3)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace σ by $\sigma(4\ 5)$, and $\sigma(4\ 5)$ is an element of A_n. Note, here we use the fact that $n \geq 5$. A_4 is not simple in particular. ■

Theorem 1.7. A_n is simple for all $n \geq 5$.

Proof. Let $1 \neq N \trianglelefteq A_n$. Suffices to show that N contains a 3-cycle, since Lemma (1.3) and (1.4) shows that we will have $N = A_n$.

Take $1 \neq \sigma \in N$ and write σ as a product of disjoint cycles. We consider three cases,

1. σ contains a cycle of length $r \geq 4$. Without loss of generality, $\sigma = (1\ 2\ 3\ \cdots\ r)\tau$. Let $\delta = (1\ 2\ 3)$, and we have

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= (r\ \cdots\ 2\ 1)(1\ 3\ 2)(1\ 2\ \cdots\ r)(1\ 2\ 3) \\ &= (2\ 3\ r).\end{aligned}$$

   This implies that N contains a 3-cycle.

2. σcontains two 3-cycles. Without loss of generality, let $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$. Let $\delta = (1\ 2\ 4)$, we have

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 2\ 3)(4\ 5\ 6)(1\ 2\ 4)\\ &= (1\ 2\ 4\ 3\ 6).\end{aligned}$$

   Thus, we are done by case 1.

3. σ contains two 2-cycles. Without loss of generality, let $\sigma = (1\ 2)(3\ 4)\tau$. Let $\delta = (1\ 2\ 3)$, we have

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3)\\ &= (1\ 4)(2\ 3) \equiv \pi.\end{aligned}$$

   Let $\epsilon = (2\ 3\ 5)$ (here we also used $n \geq 5$), we have

$$\begin{aligned}\pi^{-1}\epsilon^{-1}\pi\epsilon &= (1\ 4)(2\ 3)(2\ 5\ 3)(1\ 4)(2\ 3)(2\ 3\ 5)\\ &= (2\ 5\ 3).\end{aligned}$$

   Thus, N contains a 3-cycle.

It remains to consider σ with cycle type $(* *)$, $(* *)(* * *)$ which are not elements of A_n, and $(* * *)$ which is a 3-cycle itself. ■

Lecture 5

29 Jan. 12:00

1.4 p-groups and p-subgroups

Definition 1.14. Let p be a prime. A finite group G is a p-group if $|G| = p^n, n \geq 1$.

Theorem 1.8. If G is a p-group, then $Z(G) \neq \mathbf{1}$.

Proof. For $g \in G$, we have by orbit-stabilizer theorem,

$$|\mathrm{ccl}_G(g)||C_G(g)| = |G| = p^n.$$

So each conjugacy class has size a power of p. Since G is a disjoint union of conjugacy classes, $|G| = \#(\text{conjugacy classes of size } 1) \mod p$. It is easy to see that the conjugacy classes of size 1 are precisely the elements in the center of a group. That is, $|Z(G)| \equiv 0 \mod p$, and hence $Z(G) \neq \mathbf{1}$. ■

Corollary 1.1. The only simple p-group is C_p.

Proof. Let G be a simple p-group. Since $Z(G) \trianglelefteq G$, we have $Z(G) \neq \mathbf{1}$, so $Z(G) = G$. That is G is Abelian. We know that the only Abelian simple groups are C_p, so $G = C_p$. ■

Corollary 1.2. Let G be a p-group of order p^n. Then G has a subgroup of order p^r for all $0 < r \leq n$.

Proof. By Lemma (1.2), G has a composition series

$$\mathbf{1} \cong G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m \cong G$$

with each quotient G_{i+1}/G_i simple.

Because G is a p-group, each of the quotients is a p-group. So $G_{i+1}/G_i \cong C_p$.

Thus, $|G_i| = p^i$ for $0 \leq i \leq m = n$. ■

Lemma 1.5. For G a group, if $G/Z(G)$ is cyclic, then G is Abelian. (so in fact $G/Z(G) = \mathbf{1}$)

Proof. Let $gZ(G)$ be a generator for $G/Z(G)$, then each coset is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$.

Thus, $G = \{g^r z \mid r \in \mathbb{Z}, z \in Z(G)\}$. We check that two general elements in the group commute.

$$g^{r_1} z_1 g^{r_2} z_2 = g^{r_1+r_2} z_1 z_2 = g^{r_1+r_2} z_2 z_1 = g^{r_2} z_2 g^{r_1} z_1.$$

So G is Abelian. ■

Corollary 1.3. If $|G| = p^2$ then G is Abelian.

Proof. We have three choices for the size of the center of the group. Noting that the center cannot be trivial for a p-group. So $|Z(G)| = p$ or $|Z(G)| = p^2$.

If $|Z(G)| = p$, $|G/Z(G)| = p$, apply Lemma (1.5), and we have a contradiction.

If $|Z(G)| = p^2$, then $Z(G) = G$ so G is Abelian. ■

Note that this is not true for $|G| = p^3$.

Theorem 1.9 (Sylow Theorems). Let G be a finite group of order $p^a m$ where p is a prime with $p \nmid m$. Then

1. The set $\mathrm{Syl}_p(G) = \{P \leq G \mid |P| = p^a\}$ of Sylow p-subgroups is non-empty.
2. All elements of $\mathrm{Syl}_p(G)$ are conjugates.
3. If $n_p := \left|\mathrm{Syl}_p(G)\right|$ satisfies $n_p \equiv 1 \mod p$ and $n_p \mid |G|$ (and so $n_p \mid m$).

Corollary 1.4. If $n_p = 1$, then the unique Sylow p-subgroup is normal.

It is useful to show that the group of a certain order cannot be simple.

Proof. Let $g \in G$, and $P \in \mathrm{Syl}_p(G)$. Then $gPg^{-1} = P$ because $n_p = 1$. Thus, $P \trianglelefteq G$. ■

Example. Let $|G| = 1000 = 2^3 \cdot 5^3$. Then $n_5 \equiv 1 \mod 5$ and $n_5 \mid 8$. So $n_5 = 1$. Thus, the unique Sylow 5-subgroup is normal and of order 125. Hence, G is not simple.

Example. Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. We have $n_{11} \equiv 1 \mod 11$ and $n_{11} \mid 12$, so $n_{11} = 1$ or 12.

Suppose that G is simple. Then $n_{11} \neq 1$ (otherwise the Sylow 11-subgroup is normal) and hence $n_{11} = 12$.

Now we consider $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$. So $n_3 = 1, 4, 22$. Similarly, $n_3 \neq 1$.

Suppose $n_3 = 4$. Then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $\phi : G \to S_4$. So $\ker(\phi) \trianglelefteq G \implies \ker(\phi) = 1$ or G. But by second Sylow Theorem, the action is transitive, so the kernel must be trivial, but $132 > 24$, so ϕ cannot possibly be an injection.

Thus, $n_3 = 22$ and $n_{11=12}$. So G would have $22 \cdot (3-1)$ elements of order 3 and G has $12 \cdot (11-1) = 120$ elements of order 11. But $44 + 120 > 132 = |G|$, contradiction.

Proof of Sylow Theorems. We have $|G| = p^a m$ where p is prime and $p \nmid m$.

1. Let Ω be set of all subsets of G of order p^a. So

$$|\Omega| = \binom{p^a m}{p^a} = \frac{p^a m}{p^a} \frac{p^a m - 1}{p^a - 1} \cdots \frac{p^a m - p^a + 1}{1}$$

for $0 \leq k < p^a$, the number $p^a m - k$, the numbers $p^a m - k$ and $p^a - k$ are divisible by the same powers of p. So $|\Omega|$ is coprime to p. Let G act on $|\Omega|$ by left multiplication. That is, for $g \in G$ and $X \in \Omega$,

$$g * X = \{gx \mid x \in X\} \in \Omega.$$

For any $X \in \Omega$, we have

$$|G_X||\mathrm{orb}_G(X)| = |G| = p^a m.$$

Because $|\Omega|$ is coprime to p. We can find some X such that $|\mathrm{orb}_G(X)|$ is coprime to p. Thus, $p^a \mid |G_X|$.

On the other hand, if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$, and we have

$$G = \bigcup_{g \in G} g * X = \bigcup_{y \in \mathrm{orb}_G(x)} y.$$

So $|G| \leq |\mathrm{orb}_G(X)||X| \implies |G_x| = \frac{|G|}{|\mathrm{orb}_G(X)|} \leq |X| = p^a$.

Combining the two facts, we have $|G_X| = p^a$, i.e., $G_x \in \mathrm{Syl}_p(G)$.

2. We prove a stronger result.

   Lemma 1.6. If $P \in \mathrm{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q \leq gPg^{-1}$ for some $g \in G$.

   The lemma implies Second Sylow Theorem by taking Q a Sylow subgroup.

   Let Q act at the set of left cosets ${}^{G}/_{P}$ by left multiplication. That is, $q * gP = (qg)P$. By orbit-stabilizer Theorem, each orbit has size dividing $|Q|$, so each orbit has size 1 or a power of p.

   Since $|{}^{G}/_{P}| = m$ is coprime to p, there must exist an orbit of size 1. That is, there exists $g \in G$ such that $qgP = gP$ for all q. So $g^{-1}qg \in P$ for all $q \in Q$. So $Q \leq gPg^{-1}$.

3. Let G act on $\mathrm{Syl}_p(G)$ by conjugation. By Second Sylow Theorem, the action is transitive. Thus, orbit-stabilizer implies $n_p = \left|\mathrm{Syl}_p(G)\right| \mid |G|$.

   Now let $P \in \mathrm{Syl}_p(G)$. Then P act on $\mathrm{Syl}_p(G)$ by conjugation. The orbits have size dividing $|P| = p^a$, the size is either 1 or a power of p. So P is in an orbit of size 1.

   To show $n_p \equiv 1 \mod p$, suffices to show that $\{P\}$ is the only orbit of size one. If $\{Q\}$ is another orbit of size 1, then P normalizes Q. That is $P \leq N_G(Q)$. Note that P, Q are both Sylow p-subgroups of $N_G(Q)$.

   Thus, by Second Sylow Theorem, P and Q are conjugate in $N_G(Q)$, hence equal since $Q \trianglelefteq N_G(Q)$. Hence, $P = Q$ and $\{P\}$ is the unique orbit of size 1.

■

Lecture 6

1 Feb. 2022

1.5 Matrix Groups

For F a field (e.g. $\mathbb{C}$ or ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$), Let $GL_n(G)$ be the $n \times n$ invertible matrices with entries in F. And let $SL_n(G) = \ker(\det)$.

Let $Z \trianglelefteq GL_n(F)$ be subgroup of scalar matrices.

Definition 1.15. The *projective general linear group* is

$$PGL_n(F) = {}^{GL_n(F)}/_{Z},$$

and the *projective special linear group* is

$$PSL_n(G) = {}^{SL_n(F)}/_{Z \cap SL_n(F)} \cong {}^{Z \cdot SL_n(F)}/_{Z} \leq PGL_n(F).$$

Example. Consider $G = GL_n({}^{\mathbb{Z}}/_{p\mathbb{Z}})$. A list of n vectors in $({}^{\mathbb{Z}}/_{p\mathbb{Z}})^n$ are the

columns of some $A \in G$ if and only if they are linearly independent. Thus,

$$\begin{aligned}|G| &= (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}) \\ &= p^{1+2+\cdots+n-1}(p^n-1)(p^{n-1}-1)\cdots(p-1) \\ &= p^{\binom{n}{2}}\prod_{i=1}^{n}(p^i-1).\end{aligned}$$

So the Sylow p-subgroups have sizes $p^{\binom{n}{2}}$. Let

$$U = \left\{ \begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\} \leq G,$$

the set of upper triangular matrices with 1 on the diagonal. Then $U \in \mathrm{Syl}_p(G)$, since we have $\binom{n}{2}$ entries in U, and each can take p values.

The group $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Möbius transformations, and similarly, $PGL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ via the finite field equivalent of Möbius transformation.

Since the scalar matrices act trivially, we obtain an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 1.7. The permutation representation $PGL_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ is injective (in fact in isomorphism if $p = 2$ or $p = 3$).

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. Setting $z = 0$ gives $b = 0$. Setting $z = \infty$ gives $c = 0$. And setting $z = 1$ gives $a = d$. So it must be a scalar matrix, hence trivial in $PGL_2(\mathbb{Z}/p\mathbb{Z})$. The isomorphism can be established by considering the sizes of the groups when $p = 2$ and $p = 3$. ■

Lecture 7

3 Feb. 2022

Lemma 1.8. If p is an odd prime

$$|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{p(p-1)(p+1)}{2}.$$

Proof. From above, $|GL_2(\mathbb{Z}/p\mathbb{Z})| = p(p^2-1)(p-1)$. First we note the group homomorphism $GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ by taking the determinant is surjective. Thus, $|SL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|GL_2(\mathbb{Z}/p\mathbb{Z})|}{p-1} = p(p-1)(p+1)$.

And if a scalar matrix $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$, then $\lambda^2 \equiv 1 \mod p$, so

$$p \mid (\lambda-1)(\lambda+1) \implies \lambda \equiv \pm 1 \mod p.$$

Thus, $Z \cap SL_2(\mathbb{Z}/p\mathbb{Z}) = \{\pm I\}$, and they are distinct since $p > 2$. So we have

$$|PSL_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|SL_2(\mathbb{Z}/p\mathbb{Z})|}{2} = \frac{p(p-1)(p+1)}{2}.$$

■

Example. Let $G = PSL_2(\mathbb{Z}/5\mathbb{Z})$, then $|G| = \frac{4\cdot5\cdot6}{2} = 60$.

Let G act on $\mathbb{Z}/5\mathbb{Z} \cup \{\infty\}$ via the Möbius-like transformation. By Lemma (1.7), the permutation representation $\phi : G \to \mathrm{Sym}(\{0,1,2,3,4,\infty\})$ is injective. We claim that $\mathrm{Im}(\phi) \leq A_6$; that is, $\psi : G \to S_6 \to \{\pm 1\}$ is trivial.

Let $h \in G$ have order $2^n m$, m odd. If $\psi(h^m) = 1$, then

$$\psi(h)^m = 1 \implies \psi(h) = 1.$$

Noting that h^m has order 2^n, it suffices to show that $\psi(g) = 1$ for all $g \in G$ or order a power of 2. By Lemma (1.6), every such g belongs to a Sylow 2-subgroup.

It suffices to show that $\psi(H) = 1$ for H a particular Sylow 2-subgroup. (since $\ker(\psi)$ is normal and all Sylow subgroups are conjugate)

Take $H = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle \leq G$. We compute $\phi\left(\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3)$ and $\phi\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) = (0\ \infty)(1\ 4)$. Both of which are even permutations. Thus, $\psi(H) = 1$, and this proves the claim.

Lastly, by example sheet Q14 tells you if $G \leq A_6$ and $|G| = 60$ then $G \cong A_5$.

Property (not proved in the course).

1. $PSL_n(\mathbb{Z}/p\mathbb{Z})$ is a simple group for all $n \geq 2$ and p a prime except when $(n,p) = (2,2), (2,3)$. (finite groups of Lie type)
2. The smallest non-Abelian simple groups are $A_5 \cong PSL_2(\mathbb{Z}/5\mathbb{Z})$ of order 60 and $PSL_2(\mathbb{Z}/7\mathbb{Z}) \cong GL_3(\mathbb{Z}/2\mathbb{Z})$ of order 168.

1.6 Finite Abelian groups

Later in the course we will prove the following result.

Theorem 1.10. Every finite Abelian group is isomorphic to a product of cyclic groups.

Note. Such an isomorphism is not unique.

Lemma 1.9. If $m, n \in \mathbb{Z}_{\geq 1}$ coprime, then $C_m \times C_n \cong C_{mn}$.

Proof. Let g and h be generators of C_n and C_m. Then $(g,h) \in C_m \times C_n$ and $(g,h)^r = (g^r, h^r)$. Hence, $(g,h)^r = 1 \iff m \mid r \wedge n \mid r \iff mn \mid r$. Thus, (g,h) has order $mn = |C_m \times C_n|$. And we have $C_m \times C_n \cong C_{mn} = \langle (g,h) \rangle$. ■

Corollary 1.5. Let G be a finite Abelian group, then $G \cong C_{n_1} \times C_{n_2} \times \cdots C_{n_k}$ where n_i is a prime power.

Proof. If $n = p_1^{a_1} \cdots p_r^{a_r}$ ($p_1, \ldots, p_r$ distinct primes), then Lemma (1.5) shows $C_n \cong C_{p_1^{a_1}} \times \cdots C_{p_r^{a_r}}$. Writing each of the cyclic groups in Theorem (1.10) in this way gives the result. ■

We will prove a refinement of Theorem (1.10).

Theorem 1.11. Let G be a finite Abelian group. Then

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

for some $d_1 \mid d_2 \mid \cdots \mid d_t$.

Remark. The integers $n_1, \ldots, n_k$ in Corollary (1.5) (up to order) and $d_1, \ldots, d_t$ in Theorem (1.11) (assuming $d_1 > 1$) are uniquely determined by G. (Proof omit)

Example.

1. The Abelian groups of order 8 are C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$.
2. The Abelian groups of order 12 are $C_2 \times C_2 \times C_3$ and $C_4 \times C_3$ by Theorem (1.5), and $C_2 \times C_6$ and C_{12} by Theorem (1.11).

Definition 1.16. The *exponent* of a group G is the least integer $n \geq 1$ such that $g^n = 1 \; \forall g \in G$. That is, the lcm of all the orders of the elements of G.

Example. A_4 has exponent 6. The exponent here is greater than the biggest order of an element of the group.

Corollary 1.6. Every finite Abelian group contains an element whose order is the exponent of the group.

Proof. If $G \cong C_{d_1} \times \cdots \times C_{d_t}$ with $d_1 \mid d_2 \mid \cdots \mid d_t$, then every $g \in G$ has order dividing d_t, and if $h \in C_{d_t}$ is a generator, then $(1, \ldots, h) \in G$ has order d_t. Thus, G has exponent d_t. ■

Lecture 8

5 Feb. 2022

2 Rings

2.1 Definitions and Examples

Definition 2.1. A *ring* is a triple $(R, +, \cdot)$ consisting of a set R and two binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ satisfying the following axioms:

1. $R, +$ is an Abelian group with identity $0 = 0_R$.
2. Multiplication is associative and has an identity. i.e.

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \ \forall x, y, z \in R$$

and

$$\exists 1 = 1_R \in R \text{ s.t. } x \cdot 1 = 1 \cdot x = x \ \forall x \in R.$$

We say R is a *commutative* ring if $x \cdot y = y \cdot x \ \forall x, y \in R$. In fact, in this course, we will only consider commutative rings.

3. Distributivity: $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$ for all $x, y, z \in R$.

Remark.

1. As in case of groups, we need to check closure.
2. For $x \in R$, we write $-R$ as the inverse of x under $+$, and abbreviate $x + (-y)$ as $x - y$.
3. $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \implies 0 \cdot x = 0 \quad \forall x \in R.$
4. $$\begin{aligned} 0 = 0 \cdot x &= (1 - 1) \cdot x \\ &= 1 \cdot x + (-1) \cdot x \\ &= x + (-1) \cdot x \\ \implies (-1) \cdot x &= -x \quad \forall x \in R. \end{aligned}$$

Definition 2.2. A subset $S \subseteq R$ is a *subring* (written $S \leq R$) if it is a ring under $+$ and $\cdot$, with the same identity elements 0 and 1.

Example.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
2. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$ (ring of Gaussian integers).
3. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \leq \mathbb{R}$.
4. $\mathbb{Z}/n\mathbb{Z} = \{\text{integers mod } n\}$.
5. If R, S are rings, the ring $R \times S$ is a ring via the operations
   - $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$;
   - $(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$;
   - $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$.

   (Note: $R \times \{0\}$ is not a subring).

6. If R is a ring, a *polynomial* f over R is an expression $f = a_0 + a_1X + a_2X^2 + \cdot + a_nX^n, a_i \in R$. "$X$" is just a formal symbol.

   The degree of a polynomial is largest $n \in \mathbb{N}$ such that a_n is nonzero. We write $R[X]$ for the set of all polynomials over R.

   If $g = b_0 + b_1X + \cdots + b_mX^m$ is another polynomial, set

$$f + g = \sum_i (a_i + b_i)X^i,$$

$$f \cdot g = \sum_i (\sum_{j=0}^{i} a_j b_{i-j})X^i.$$

   Then $R[X]$ is a ring with identities 0_R and 1_R which are constant polynomials.

   A *monic polynomial* is one such that the leading coefficient $a_n = 1_R$.

   We can identify R with subring of $R[X]$ of constant polynomials (i.e. $\sum_i a_iX^i, a_i = 0 \ \forall i > 0$).

Definition 2.3. An element $r \in R$ is a *unit* if it has an inverse under multiplication, i.e. $\exists s \in R$ s.t. $s \cdot r = 1$.

The units in R form a group $(R^\times, \cdot)$ under multiplication.

Example.

- $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$

Definition 2.4. A *field* is a ring with $0 \neq 1$, such that every non-zero element is a unit.

Example. $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$ with p prime.

Remark. If R is a ring with $0 = 1$, then $x = 1 \cdot x = 0 \cdot x = 0$ for all $x \in R$. And $R = \{0\}$ is the *trivial ring*.

Proposition 2.1. Let $f, g \in R[X]$. Suppose the leading coefficient of g is a unit. Then there exist $q, r \in R[X]$ such that

$$f(x) = q(x)g(x) + r(x) \text{ where } \deg(r) < \deg(g).$$

Proof. Induction on $n = \deg(f)$. Write

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \qquad a_n \neq 0$$
$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_0. \qquad b_m \in R^\times$$

If $n < m$, then put $q = 0, r = f$, and we are done.

Otherwise, we have $n \geq m$, and we set

$$f_1(X) = f(X) - a_n b_m^{-1} g(X) X^{n-m}$$

because b_m is a unit. The coefficient of X^n is $a_n - a_n b_m^{-1} b_m = 0$. Thus, $\deg(f_1) < n$. By inductive hypothesis $\exists q_1, r \in R[X]$ such that

$$f_1(X) = q_1(X) g(X) + r(X), \text{ where } \deg(r) < \deg(g).$$

Therefore,

$$f(X) = (q_1(X) + a_n b_m^{-1} X^{n-m}) g(X) + r(X).$$

■

Remark. We often work with polynomials over a field, then we only need the assumption that $g \neq 0$.

Example.

1. If R is a ring and X a set, then the set of all functions $X \to R$ is a ring under point-wise operations. That is,

$$(f + g)(x) = f(x) + g(x);$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

   More interesting examples will appear as subrings. For example, the continuous functions from $\mathbb{R} \to \mathbb{R}$ and the polynomial functions $\mathbb{R} \to \mathbb{R}$ which is $\mathbb{R}[X]$.

2. Power series ring. $R[\![X]\!] = \{a_0 + a_1 X + a_2 X^2 + \cdots \mid a_i \in \mathbb{R}\}$ with the same operation as the polynomial. (you should not think this as infinite sum of elements, but a formal object instead)

3. Laurent polynomials.

$$R[X, X^{-1}] = \{\sum_{i \in \mathbb{Z}} a_i X^i \mid a_i \in R, a_i \text{ is non-zero for finitely many } i\}.$$

Lecture 9

8 Feb. 2022

2.2 Homomorphisms, Ideals and Quotients

Definition 2.5. Let R and S be rings. A function $\phi : R \to S$ is a *ring homomorphism* if

1. $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \quad \forall r_1, r_2 \in R$,
2. $\phi(r_1 \cdot r_1) = \phi(r_1) \cdot \phi(r_2) \quad \forall r_1, r_2 \in R$,
3. $\phi(1_R) = 1_S$.

A ring homomorphism that is also a bijection is called an *isomorphism*.

The *kernel* of ϕ is $\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$.

Lemma 2.1. A ring homomorphism $\phi : R \to S$ is injective if and only if $\ker(\phi) = \{0_R\}$.

Proof. $\phi : (R, +) \to (S, +)$ is also a group homomorphism. And the result follows from the corresponding result from groups. ■

Definition 2.6. A subset $I \subseteq R$ is an *ideal*, written $I \trianglelefteq R$, if

1. I is a subgroup of $(R, +)$;
2. if $r \in R$ and $x \in I$, then $rx \in I$.

We say I is *proper* if $I \neq R$.

Lemma 2.2. If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal of R.

Proof. Again, $\phi : (R, +) \to (S, +)$ is a group homomorphism between the additive groups. So $\ker(\phi)$ is a subgroup of $(R, +)$.

If $r \in R$ and $x \in \ker(\phi)$, then

$$\phi(rx) = \phi(r)\phi(x) = \phi(r) \cdot 0_S = 0_S \implies rx \in \ker(\phi).$$

■

Remark. If I contains a unit, then $1_R \in I$ because ideal is closed by multiplication with any element in R; hence, $I = R$. Thus, if I is a proper ideal, $1_R \notin I$, so I is not a subring of R.

Lemma 2.3. The ideals in $\mathbb{Z}$ are $n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$, for $n = 0, 1, 2, \ldots$.

Proof. Certainly, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Let $I \trianglelefteq \mathbb{Z}$ be a non-zero ideal, and let n be the smallest positive integer in I. Then $n\mathbb{Z} \subseteq I$. If $m \in I$, then write $m = qn + r$ where $q, r \in \mathbb{Z}$, and $0 \leq r < n$

by division algorithm. Then $r = m - qn \in I$ contradicts the minimality of n unless $r = 0$. Then we have $m \in n\mathbb{Z}$; i.e. $I = n\mathbb{Z}$. ■

Definition 2.7. For $a \in R$, write $(a) = \{ra \mid r \in R\} \trianglelefteq R$. This is the *ideal generated by* a.

Generally, if $a_1, \ldots, a_n \in R$, we write *the ideal generated by* $a_1, \ldots, a_n$ as

$$(a_1, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \ldots + r_na_n \mid r_i \in R\} \trianglelefteq R.$$

Definition 2.8. Let $I \trianglelefteq R$, we say I is *principal* if $I = (u)$ for some $u \in R$.

Theorem 2.1. If $I \trianglelefteq R$, then the set ${}^{R}\!/_{I}$ of cosets of I in $(R, +)$ forms a ring (called the *quotient ring*) with the operations

$$(r_1 + I) + (r_2 + I) = r_1 + r_2 + I,$$
$$(r_1 + I) \cdot (r_2 + I) = r_1 \cdot r_2 + I$$

and $0_{R/I} = O_R + I$, $1_{R/I} = 1_R + I$.

Moreover, the map $R \to {}^{R}\!/_{I}, r \mapsto r + I$ is a ring homomorphism (called the *quotient map*) with kernel I.

Proof. We already know that $({}^{R}\!/_{I}, +)$ is a group. We want to show that the multiplication is well-defined. If $r_1 + I = r_1' + I$, $r_2 + I = r_2' + I$, then for some $a_1, a_2 \in I$, $r_1' = r_1 + a_1$, $r_2' = r_2 + a_2$. Then we have

$$\begin{aligned} r_1'r_2' &= (r_1 + a_1)(r_2 + a_2) \\ &= r_{1r_2+r_1}a_2 + r_2a_1 + a_1a_2. \end{aligned}$$

Thus, $r_1r_2 + I = r_1'r_2' + I$.

The remaining properties for ${}^{R}\!/_{I}$ follows from those properties for R. And the quotient map is clearly a ring homomorphism from the definitions of the quotient ring. ■

Example.

1. $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ with quotient ring ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. To be precise, ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ has elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots$. Addition and multiplication are carried out mod$n$.
2. Consider $(X) \trianglelefteq \mathbb{C}[X]$, the polynomials with constant term 0.

   If $f(X) = a_nX^n + \cdots + a_1X + a_0, a_i \in \mathbb{C}$, then $f(X) + (X) = a_0 + (X)$. There is a bijection from ${}^{\mathbb{C}[X]}\!/_{(X)} \to \mathbb{C}, f(X) + (X) \mapsto f(0)$.

   These maps are ring homomorphisms. Thurs, ${}^{\|C[X]}\!/_{(X)} \cong \mathbb{C}$.
3. Consider $(X^2 + 1) \trianglelefteq \mathbb{R}[X]$,

$$ {}^{\mathbb{R}[X]}\!/_{(X^2+1)} = \{f(X) + (X^2 + 1) \mid f(X) \in \mathbb{R}[X]\}.$$

By Proposition (2.1), $f(X) = q(X)(X^2+1) + r(X)$ with $\deg r < 2$, i.e. $r(X) = a + bX, a, b \in \mathbb{R}$. Thus,

$$\mathbb{R}/(X^2+1) = \{a + bX + (X^2+1) \mid a, b \in \mathbb{R}\}.$$

If $a + bX + (X^2+1) = a' + b'X + (X^2+1)$, then

$$a - a' + (b - b')X = g(X)(X^2+1).$$

Comparing degrees, we see $g(x) = 0$ and $a = a'$ and $b = b'$. Consider the bijection

$$\begin{aligned} \phi\colon \mathbb{R}[X]/X^2+1 &\longrightarrow \mathbb{C} \\ a + bX + (X^2+1) &\longmapsto a + bi. \end{aligned}$$

We show that ϕ is a ring homomorphism. It preserves addition and maps $1 + (X^2+1)$ to 1. We show that it preserves multiplication.

$$\begin{aligned} &\phi((a + bX + (X^2+1))(c + dX + (X^2+1))) \\ =&\phi((a+bX)(c+dX) + (X^2+1)) \\ =&\phi(ac + (ad+bc)X + bd(X^2+1) - bd + (X^2+1)) \\ =&ac - bd + (ad+bc)i \\ =&(a+bi)(c+di) \\ =&\phi(a + bX + (X^2+1))\phi(c + dX + (X^2+1)). \end{aligned}$$

Thus, $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.

Lecture 10

10 Feb. 2022

Theorem 2.2 (First Isomorphism Theorem). Let $\phi : R \to S$ be a ring homomorphism, then $\ker(\phi) \trianglelefteq R$, $\mathrm{Im}(\phi) \leq S$ and there exists isomorphism $R/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Proof. We already showed that $\ker(\phi) \trianglelefteq R$ in Lemma (2.2), and $\mathrm{Im}(\phi)$ is a subgroup of $(S, +)$ by First Isomorphism Theorem for groups. So just need to show that it's closed under multiplication and contains 1_S.

We have $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \mathrm{Im}(\phi)$ and $1_S = \phi(1_R) \in \mathrm{Im}(\phi)$. Thus, $\mathrm{Im}(\phi)$ is a subring of S.

Let $K = \ker(\phi)$, and define

$$\begin{aligned} \Phi\colon R/K &\longrightarrow \mathrm{Im}(\phi) \\ r + K &\longmapsto \phi(r) \end{aligned}.$$

Again, by the First Isomorphism Theorem for groups, this is well-defined, a bijection and group homomorphism under addition.

Also, $\Phi(1_R + K) = \phi(1_R) = 1_S$, and

$$\begin{aligned}\Phi((r_1 + K)(r_2 + K)) &= \Phi(r_1 r_2 + K) \\ &= \phi(r_1 r_2) = \phi(r_1)\phi(r_2) \\ &= \Phi(r_1 + K)\Phi(r_2 + K).\end{aligned}$$

Thus, Φ is an isomorphism of rings. ■

Theorem 2.3 (Second Isomorphism Theorem). Let $R \leq S$ and $J \trianglelefteq S$. Then $R \cap J \trianglelefteq R$, $R + J = \{r + a \mid r \in R, a \in S\} \leq S$ and

$$\frac{R}{R \cap J} \cong \frac{R + J}{J} \leq \frac{S}{J}.$$

Proof. By Second Isomorphism Theorem of groups, $R + J$ is a subgroup of $(S, +)$, and we have $1_S = 1_S + 0_S \in R + J$.

If $r_1, r_2 \in R$ and $a_1, a_2 \in J$, we have

$$\begin{aligned}(r_1 + a_1)(r_2 + a_2) &= r_1 r_2 + r_1 a_2 + r_2 a_1 + a_1 a_2 \\ &= r_1 r_2 + a.\end{aligned}$$

Thus, $R + S \leq S$.

Let $\phi : R \to {}^{S}\!/_{J}, r \mapsto r + J$. Thus is the composition of the inclusion $R \leq S$, and the quotient map $S \to {}^{S}\!/_{J}$. We have

$$\begin{aligned}\ker(\phi) &= \{r \in R \mid r + J = J\} = R \cap J \trianglelefteq R \\ \mathrm{Im}(\phi) &= \{r + J \mid r \in R\} = \frac{R + J}{J} \leq \frac{S}{J}.\end{aligned}$$

And by First Isomorphism Theorem, we have

$$\frac{R}{R \cap J} \cong \frac{R + J}{J}.$$

■

Note. Let $I \trianglelefteq R$, there exists a bijection

$$\begin{aligned}\{\text{Ideals of } {}^{R}\!/_{I}\} &\longleftrightarrow \{\text{Ideals of } R \text{ containing } I\}, \\ K &\longmapsto \{r \in R \mid r + I \in K\}, \\ {}^{J}\!/_{I} &\longmapsfrom J.\end{aligned}$$

Theorem 2.4 (Third Isomorphism Theorem). Let $I \trianglelefteq R, J \trianglelefteq R$ with $I \subseteq J$, then ${}^{J}\!/_{I} \trianglelefteq {}^{R}\!/_{I}$, and

$$\frac{{}^{R}\!/_{I}}{{}^{J}\!/_{I}} \cong \frac{R}{J}.$$

Proof. Consider

$$\begin{aligned}\phi\colon {}^{R}\!/_{I} &\longrightarrow {}^{R}\!/_{J}\\ r+I &\longmapsto r+J\end{aligned}$$

This is a surjective ring homomorphism. (well-defined since $I \subseteq J$) And

$$\ker(\phi) = \{r + I \mid r \in J\} = {}^{J}\!/_{I} \trianglelefteq {}^{R}\!/_{I}.$$

Apply First Isomorphism Theorem, and we are done. ■

Example. There is a surjective ring homomorphism

$$\begin{aligned}\phi\colon \mathbb{R}[X] &\longrightarrow \mathbb{C}\\ f(X) = \sum_{n=1}^{\infty} a_n X^n &\longmapsto f(i) = \sum_{n=1}^{\infty} a_n i^n\end{aligned}$$

Proposition (2.1) implies that $\ker(\phi) = (X^2 + 1)$.

First Isomorphism Theorem tells us ${}^{\mathbb{R}[X]}\!/_{(X^2+1)} \cong \mathbb{C}$.

Example. Let R a ring, there is a unique ring homomorphism $i : \mathbb{Z} \to R$, given by

$$\begin{aligned}0 &\longmapsto 0_R\\ 1 &\longmapsto 1_R\\ n &\longmapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}\\ -n &\longmapsto -(\underbrace{1_R + \cdots + 1_R}_{n \text{ times}}).\end{aligned}$$

Since $\ker(i) \trianglelefteq \mathbb{Z}$, we have $\ker(i) = n\mathbb{Z}$ for some $n = 0, 1, 2, \ldots$.

By First Isomorphism Theorem,

$${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathrm{Im}(i) \leq R.$$

Definition 2.9. We call n the *characteristic* of R.

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ all have characteristic 0, and ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}, {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]$ have characteristic p.

2.3 Integral Domains, Maximal Ideals and Prime Ideals

Definition 2.10. An *integral domain* is a ring with $0 \neq 1$, and such that for $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

A *zero-divisor* in a ring R is a non-zero element $a \in R$ such that $ab = 0$ for some $0 \neq b \in R$.

So an integral domain is a ring with no zero-divisors.

Example.

1. All fields are integral domains. (if $ab = 0$ with $b \neq 0$, multiply by b^{-1} to get $a = 0$)
2. Any subring of an integral domain is an integral domain. E.g., $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Z}[i] \leq \mathbb{C}$.
3. $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain since $(1, 0) \cdot (0, 1) = (0, 0)$.

Lemma 2.4. If R is an integral domain, so is $R[X]$.

Proof. Write $f(x) = a_m X^m + \cdots + a_1 X + a_0 \quad a_m \neq 0$. Then
$g(x) = b_n X^n + \cdots + b_1 X + b_0 \qquad b_n \neq 0$

$$f(x)g(x) = a_m b_n X^{n+m} + \cdots .$$

We know $a_m b_n \neq 0$ since R is an integral domain. Then $\deg(f \cdot g) = m + n$ and $f \cdot g$ is non-zero. ■

Lecture 11

12 Feb. 2022

Lemma 2.5. Let R be an integral domain, and $f \neq 0 \in R[X]$. Let $\text{Roots}(f) = \{a \in R \mid f(a) = 0\}\}$. Then

$$|\text{Roots}(f)| \leq \deg(f).$$

Proof. Example sheet. ■

Theorem 2.5. Let F be a field. Then any finite subgroup of $G \leq (F^\times, \cdot)$ is cyclic.

Proof. G is a finite Abelian group because we are working with a commutative ring. If G is not cyclic, then by Structure Theorem for Finite Abelian Groups, $\exists H \leq G$ such that $H \cong C_{d_1} \times C_{d_1}$ for some $d_1 \geq 2$. But then the polynomial

$$f(X) = X^{d_1} - 1 \in F[X]$$

has degree d_1, and has d_1^2 roots contradicting the above lemma. ■

Example. $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. That is, it has a *primitive root*.

Proposition 2.2. Any finite integral domain is a field.

Proof. Let R be a finite integral domain. Let $a \neq 0 \in R$. Consider the map

$$\begin{aligned} \phi \colon R &\longrightarrow R \\ x &\longmapsto ax \end{aligned}.$$

We claim that it is injective. If $\phi(x) = \phi(y)$, then $a(x-y) = 0 \implies x = y$ because R is an integral domain and a is nonzero.

Thus, ϕ is injective, and hence surjective since R is finite. So there exists $b \in R$ such that $ab = 1$. That is, a is a unit. Thus, R is a field. ■

Theorem 2.6. Let R be an integral domain. Then there exists a field F such that

1. $R \leq F$;
2. Every element of F can be written in the form ab^{-1} where $a, b \in R$ with $b \neq 0$.

F is called the *field of fractions* of R.

Proof. Consider the set $S = \{(a,b) \mid b \neq 0\}\}$ and the equivalence relation $\sim$ given by $(a,b) \sim (c,d) \iff ad - bc = 0$.

Clearly the relation is reflexive and symmetric.

For transitivity, if $(a,b) \sim (c,d) \sim (e,f)$ then

$$(ad)f = (bc)f = b(cf) = b(de) \implies d(af - be) = 0.$$

Since R is an integral domain and $d \neq 0$, this means

$$af - be = 0 \implies (a,b) \sim (e,f).$$

Let $F = {}^{S}/_{\sim}$ and write $\frac{a}{b}$ for $[(a,b)]$. We define the following operations to make F a field.

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}. \end{aligned}$$

Can be checked that these operations are well-defined and make F into a ring with $0_F = \frac{0_R}{1_R}$ and $1_F = \frac{1_R}{1_R}$.

If $\frac{a}{b} \neq \frac{b}{a}$, then $a \neq 0_R$. And we have

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1_R}{1_R} = 1_F.$$

So F is a field.

We can identify R with the subring $\{\frac{r}{1_R} \mid r \in R\}$. We also have $\frac{a}{b} = a \cdot b^{-1}$. ■

Example.

1. $\mathbb{Z}$ is an integral domain with field of fractions $\mathbb{Q}$.
2. $\mathbb{C}[X]$ has field of fractions $\mathbb{C}(X)$ called the field of rational functions in X.

Definition 2.11. An ideal $I \trianglelefteq R$ is *maximal* is $I \neq R$ and if $I \subseteq J \trianglelefteq R$, then $J = I$ or $J = R$.

Lemma 2.6. A (non-zero) ring R is a field if and only if its only ideals are $\{0\}$ are R.

Proof. $\implies$ direction. If $0 \neq I \trianglelefteq R$ then I contains a unit and hence $I = R$.

$\impliedby$ direction. If $0 \neq x \in R$, then the ideal (x) is non-zero, hence $(x) = R$, and there exists $y \in R$ such that $xy = 1$. That is x is a unit. ■

Proposition 2.3. Let $I \trianglelefteq R$ be an ideal. I is maximal if and only if R/I is a field.

Proof. R/I is a field.

$\iff$ I/I and R/I are the only ideals in R/I.

$\iff$ I and R are the only ideals in R containing I.

$\iff$ $I \trianglelefteq R$ is maximal. ■

Definition 2.12. An ideal $I \trianglelefteq R$ is *prime* if $I \neq R$ and whenever $a, b \in R$ with $ab \in I$, we have $a \in I$ or $b \in I$.

Example. The ideals $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a prime ideal if and only if $n = 0$ or $n = p$ is a prime number.

If $ab \in p\mathbb{Z}$ then $p \mid ab$, so $p \mid a$ or $p \mid b$. So $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Conversely, if $n = uv$ with $u, v > 1$, then $uv \in n\mathbb{Z}$, but $u \notin n\mathbb{Z}$ and $v \notin n\mathbb{Z}$.

Proposition 2.4. Let $I \trianglelefteq R$ be an ideal of the ring R. Then I is prime $\iff$ R/I is an integral domain.

Proof. I is prime

$\iff$ Whenever $a, b \in R$ with $a, b \in I$, we have $a \in I$ or $b \in I$.

$\iff$ Whenever $a+I, b+I \in R/I$ with $(a+I)(b+I) = 0+I$, we have $a+I = 0+I$ or $b + I = 0 + I$.

$\iff$ R/I is an integral domain. ■

Remark. Proposition (2.4) and (2.3) show that I maximal $\implies$ I prime ideal.

Lecture 12

15 Feb. 2022

Remark. If $\text{char}(R) = n$, then $\mathbb{Z}/n\mathbb{Z} \leq R$. So if R is an integral domain, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. So $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a prime ideal, and we have $n = 0$ or $n = p$ a prime.

In particular, a field has characteristic 0 (and so contains $\mathbb{Q}$) or has characteristic p (and contains $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$).

2.4 Factorization in Integral Domains

In this section, R is always an integral domain.

Definition 2.13.

1. $a \in R$ is a *unit* if $\exists b \in R$ with $ab = 1$. (equivalently, $(a) = R$) And we write the units in R as $R^\times$.
2. $a \in R$ divides $b \in R$ (written $a \mid b$) if $\exists c \in R$ such that $b = ac$. (equivalently, $(b) \subseteq (a)$)
3. $a, b \in R$ are *associates* if $a = bc$ for some unit $c \in R$. (equivalently, $(b) = (a)$)
4. $r \in R$ is *irreducible* if $r \neq 0$, r is not a unit, and $r = ab \implies a$ or b is a unit.
5. $r \in R$ is *prime* if $r \neq 0$ and r is not a unit, and $r \mid ab \implies r \mid a$ or $r \mid b$.

Note. These properties depend on ambient ring R. For example,

1. 2 is prime and irreducible in $\mathbb{Z}$, but not in $\mathbb{Q}$.
2. $2X$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{Z}[X]$.

Lemma 2.7. $(r) \trianglelefteq R$ is a prime ideal if and only if $r = 0$ or r is prime.

Proof. $\implies$ direction. Suppose (r) is prime and $r \neq 0$. Since prime ideals are proper, $(r) \neq R$, so $r \notin R^\times$. If $r \mid ab$, then $ab \in (r)$, so $a \in (r)$ or $b \in (r)$, and we have $r \mid a$ or $r \mid b$. That is, r is prime.

$\impliedby$ direction. $\{0\} \trianglelefteq R$ is a prime ideal since R is an integral domain. Let $r \in R$ be a prime. $(r) \neq R$ since $r \notin R^\times$. If $ab \in (r)$, then $r \mid ab$ so $r \mid a$ or $r \mid b$. That is $a \in (r)$ or $b \in (r)$; that is, (r) is a prime ideal. ■

Lemma 2.8. If r is a prime element, then it is irreducible.

Proof. Since r is prime, $r \neq 0$ and $r \notin R^\times$. Suppose $r = ab$. Then $r \mid ab$ so $r \mid a$ or $r \mid b$. Assume $r \mid a$, so $a = rc$ for some $c \in R$. Then $r = ab = rcb \implies r(1 - bc) = 0 \implies bc = 1$ since R is an integral domain and $r \neq 0$. That is, b is a unit. ■

The converse does not hold in general.

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$ which is isomorphic to ${}^{\mathbb{Z}[X]}/_{(X^2+5)}$. R is a subring of a field, so an integral domain.

Define a function $N : R \to \mathbb{Z}$, $a + b\sqrt{-5} \mapsto a^2 + 5b^2$.

Note that $N(z_1 z_2) = N(z_1)N(z_2)$. We claim that $R^\times = \{\pm 1\}$.

Proof. If $r \in R^\times$, i.e. $rs = 1$ for some $s \in R$. Then

$$N(r)N(s) = N(1) = 1 \implies N(r) = 1.$$

But the only integer solutions to the equation $a^2 + 5b^2 = 1$ are $(\pm 1, 0)$. ■

Next we note that $2 \in R$ is irreducible.

Proof. Suppose $2 = rs$ with $r, s \in R$. Then $4 = N(2) = N(r)N(2)$. Since the equation $a^2 + 5b^2 = 2$ has no integer solutions, R has no elements of norm 2. Thus, $N(r) = 1$ and $N(s) = 4$ or vice versa. But, $N(r) = 1 \implies r$ is a unit. ■

Similarly, $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible. (as these are the elements of norm 3)

But we have $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3 = 6$, so $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$. But we know $2 \nmid 1 + \sqrt{-5}$ and $2 \nmid 1 - \sqrt{-5}$. Check by taking norms, we have $4 \nmid 6$. Thus, 2 is not prime in R.

Remark.

1. In general, irreducible elements don't have to be prime.
2. $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ gives two different factorization into irreducibles. Since $R^\times = \{\pm 1\}$, the irreducibles are not associates, so they are really different factorizations.

Definition 2.14. An integral domain R is a *principal ideal domain* (PID) if any ideal $I \trianglelefteq R$ is principal, i.e. $I = (r)$ for some $r \in R$.

Example. $\mathbb{Z}$ is a PID as proved in previous lecture.

Proposition 2.5. Let R be a PID. Then every irreducible element of R is a prime.

Proof. Let $r \in R$ be irreducible. If $r \mid ab$ and $r \nmid a$, Because R is a PID, $(a, r) = (d)$ for some $d \in R$. In particular, $r = cd$ for some $c \in R$. Since r is irreducible, either c or d is a unit.

If c a unit, then $(a, r) = (r)$. So $r \mid a$, contradiction.

If d a unit, then $(a, r) = R$. So exists $s, t \in R$ such that $sa + tr = 1$, then

$$b = sab + rrb,$$

and since $r \mid ab$, we must have $r \mid b$. Thus, r is a prime. ■

Lecture 13

17 Feb. 2022

R will always be an integral domain in this section.

Lemma 2.9. Let R be a PID, and $0 \neq r \in R$, then r irreducible $\iff$ (r) is a maximal ideal.

Proof. $\implies$ $r \notin R^\times$ so $(r) \neq R$. Suppose $(r) \subseteq J \subseteq R$ with $J \trianglelefteq R$. Because R is a PID, $J = (a)$ for some $a \in R$. So $r = ab$ for some $b \in R$. Since r is irreducible, either $a \in R^\times \implies J = R$ or $b \in R^\times \implies J = (r)$. So (r) is maximal.

$\impliedby$ (true for general integral domain) $(r) \neq R$ so $r \notin R^\times$. Suppose $r = ab$, then $(r) \subseteq (a) \subseteq R$. Since (r) is maximal, either $(a) = (r) \implies b \in R^\times$ or $(a) = R \implies a \in R^\times$. Thus, r is irreducible. ■

Remark.

1. " $\impliedby$ " holds without assuming R a PID.
2. Let R be a PID, $0 \neq r \in R$, then (r) maximal $\iff$ r irreducible $\iff$ r prime $\iff$ (r) prime. Thus, there is a bijection between non-zero prime ideals and non-zero maximal ideals.

Definition 2.15. An integral domain is a *Euclidean domain* (ED) if there is a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ (a Euclidean function) such that

1. If $a \mid b$, then $\phi(a) \leq \phi(b)$;
2. If $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ with $a = bq + r$ and either $r = 0$, or $\phi(r) < \phi(b)$.

Example. $\mathbb{Z}$ is an ED with Euclidean function $\phi(n) = |n|$.

Proposition 2.6. If R is a Euclidean domain, then it is a principal ideal domain. (i.e. ED $\implies$ PID)

Proof. Let R have Euclidean function $\phi : R \setminus \{0\} \to \mathbb{Z}$.

Let $I \trianglelefteq R$ be a non-zero ideal. Choose $b \in I \setminus \{0\}$ with $\phi(b)$ minimal, then $(b) \subseteq I$. For $a \in I$, write $a = bq + r$ with $r, q \in R$ and either $r = 0$ or $\phi(r) < \phi(b)$. Since $r = bq - a \in I$, it cannot have $\phi(r) < \phi(b)$ by choice of b. Thus, $a = bq \in (b)$, and hence $I = (b)$. ■

Remark. We only used (2) here, but property (1) allows us to describe the units in R as

$$R^\times = \{u \in R \setminus \{0\} \mid \phi(a) = \phi(1)\}.$$

In fact, if you can find a function satisfying property (2), you can find another Euclidean function satisfying both properties.

Example.

1. If F is a field, $F[X]$ is an ED with Euclidean function $\phi(f) = \deg f$ with $f \in F[X]$.
2. $R = \mathbb{Z}[i]$ is an ED with Euclidean function $\phi(a+ib) = N(a+ib) = a^2+b^2$. Since $N(z_1z_2) = N(z_1)N(z_2)$, property (1) holds.

   For property (2), let $z_1, z_2 \in \mathbb{Z}[i]$ with $z_2 \neq 0$. Consider $\frac{z_1}{z_2} \in \mathbb{C}$. This has distance less than 1 from the nearest element in $\mathbb{Z}[i]$. That is, exists $q \in \mathbb{Z}[i]$ s.t. $\left|\frac{z_1}{z_2} - q\right| < 1$.

   Set $r = z_1 - z_2q \in \mathbb{Z}[i]$. Then $z_1 = z_2q + r$, and

$$\phi(r) = |r|^2 = |z_1 - z_2q|^2 < |z_2|^2 = \phi(z_2).$$

Thus, we have $\mathbb{Z}[i]$ and $F[X]$ for F a field are PIDs.

Example. Let A be an $n \times n$ matrix over a field F. Let

$$I = \{f \in F[X] \mid f(A) = 0\}.$$

If $f, g \in I$, then $(f-g)(A) = f(A)-g(A) = 0$. So $f-g \in I$, and I is a subgroup under addition.

If $f \in F[x], g \in I$, then $(f \cdot g)(A) = f(A) \cdot g(A) = 0$. So $f \cdot g \in I$, and I is closed under addition by elements of the ring.

Thus, $I \in F[X]$ is an ideal, and $I = (f)$ for some $f \in F[X]$ since $F[X]$ is PID. We may assume f is monic upon multiplying by a unit in F.

Thus, for $ginF[X]$ such that $g(A) = 0 \iff g \in I \iff g \in (f)$. That is, $f \mid g$, so f is the minimal polynomial of A.

Example (Field of 8). Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

Let $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$. If $f(X) = g(X)h(X)$ with $g, h \in \mathbb{F}_2[X]$ and $\deg g, \deg h > 0$. Because $\deg(gh) = \deg g + \deg h$, then either $\deg g = 1$ or $\deg f = 1$. And so f has a root. But $f(0) = f(1) = 1 \neq 0$. Thus, f is irreducible.

Since $\mathbb{F}_2[X]$ is a PID, $(f) \trianglelefteq \mathbb{F}_2[X]$ is a maximal ideal. Hence, $\mathbb{F}_2[X]/(f)$ is a field. And

$$\mathbb{F}_2[X]/(f) = \{aX^2 + bX + c \mid a, b, c \in \mathbb{F}_2\},$$

so it is a field of order 8 by checking different a, b, c gives distinct elements.

Lecture 14

19 Feb. 2022

Example. $\mathbb{Z}[X]$ is not a PID. Consider $I = (2, X) \trianglelefteq \mathbb{Z}[X]$, then

$$\begin{aligned} I &= \{2f_1(X) + Xf_2(X) \mid f_1, f_2 \in \mathbb{Z}[X]\} \\ &= \{f \in \mathbb{Z}[X] \mid f(0) \text{ is even}\}. \end{aligned}$$

Suppose otherwise that $I = (f)$ for some $f \in \mathbb{Z}[X]$. So $2 = fg$ for some $g \in \mathbb{Z}[X]$. Thus, $\deg f = \deg g = 0$, and $f \in \mathbb{Z}$. So $f = \pm 1$ of $f = \pm 2$. Thus, $I = \mathbb{Z}[X]$ or $I = 2\mathbb{Z}[X]$. Contradiction for both cases.

Definition 2.16. An integral domain is a *unique factorization domain* (UFD) if

1. Every non-zero, non-unit element is a product of irreducibles.
2. If $p_1 \cdots p_m = q_1 \cdots q_n$ where p_i, q_i are irreducible, then $m = n$ and we can reorder so that p_i is an associate of q_i for all $i = 1, \ldots, n$.

We want to show that PID $\implies$ UFD.

Proposition 2.7. Let R be an integral domain satisfying (1) in definition of UFD. Then R is UFD if and only if every irreducible is prime.

Proof. " $\implies$ " Suppose $p \in R$ is irreducible, and $p \mid ab$. Then $ab = pc$ for some $c \in R$. Writing a, b, c as products of irreducibles, it follows from (2) that $p \mid a$ or $p \mid b$. Thus, p is prime.

" $\impliedby$ " Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ with p_i, q_i irreducible. Since p_1 is prime, and $p_1 \mid q_1 \cdots q_n$, we have $p_1 \mid q_i$ for some i. Upon reordering, we have $p_1 \mid q_1$. That is, $q_1 = p_1 u$ for some $u \in R$. But q_1 is irreducible, and p_1 not a unit. Thus, p_1, q_1 are associates. Cancelling p_1 gives $p_2 \cdots p_m = u q_2 \cdots q_n$. Result then follows by induction. ∎

Lemma 2.10. Let R be a PID, and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a nested sequence of ideals, then $\exists N \in \mathbb{N}$ such that $I_n = I_{n+1}$ for all $n \geq N$. (Rings satisfying the "ascending chain condition" is called *Noetherian Rings*)

Proof. Let $I = \bigcup_{i=1}^{\infty} I_i$, and this is an ideal in R. (See example sheet 2)

Since R is a PID, we have $I = (a)$ for some $a \in R$. Then $a \in \bigcup_{i=1}^{\infty} I_i$, so $a \in I_N$ for some N.

Then for any $n \geq N$, we have

$$(a) \subseteq I_N \subseteq I_n \subseteq I = (a),$$

and so $I_n = I$. ∎

Theorem 2.7. If R is a principal ideal domain, then R is a unique factorization domain. (i.e. PID $\implies$ UFD)

Proof. We check (1) and (2) in the definition of UFD.

1. Let $0 \neq x \in R$ not a unit. Suppose that x is not a product of irreducibles. Then x is not irreducible. So we can write $x = x_1 y_1$ where x_i, y_i are not units. Then either x_1 or y_1 is not a product of irreducible, say x_1. We have $(x) \subseteq (x_1)$, and the inclusion is strict since y_1 is not a unit.

   Now write $x_1 = x_2 y_2$ where x_2, y_2 are not units, and ad infinitum we get

   $$(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots,$$

   which is a contradiction to Lemma (2.10).

2. By Proposition (2.7), it suffices to show irreducibles are primes. Conclude by Proposition (2.5).

■

Example. ED $\implies$ PID $\implies$ UFD $\implies$ Integral Domains.

1. $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain.
2. $\mathbb{Z}[\sqrt{-5}]$ is an integral domain that is not a UFD.
3. $\mathbb{Z}[X]$ is a UFD that is not a PID.
4. $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a PID but not an ED. (It will be proved in Part II Number Fields)
5. $\mathbb{Z}[i]$ is an ED.

Definition 2.17. R an integral domain, then

1. $d \in R$ is a *greatest common divisor* of $a_1, \ldots, a_n \in R$ (written as $d = \gcd(a_1, \ldots, a_n)$) if $d \mid a_i$ for all i and if $d' \mid a_i$ for all i, then $d' \mid d$;
2. $m \in R$ is a *least common multiple* of $a_1, \ldots, a_n \in R$ (written as $m = \operatorname{lcm}(a_1, \ldots, a_n)$) if $a_i \mid m$ for all i and if $a_i \mid m'$ for all i, then $m \mid m'$.

Both gcd and lcm (when they exist) are unique up to associates.

Proposition 2.8. In a UFD, both gcd and lcm exist.

Proof. Write $a_i = u_i \prod_j p_j^{i,j}$ for all $1 \leq i \leq n$, where u_i is a unit, the p_j are irreducible which are not associates of each other and $n_{i,j} \in \mathbb{Z}_{\geq 0}$. We claim that $d = \prod_j p_j^{m_j}$ where $m_j = \min_{1 \leq i \leq n} n_{i,j}$ is the gcd of $a_i, \ldots, a_n$.

Certainly, $d \mid a_i$ for all i. If $d' \mid a_i$ for all i, then writing $d' = u \prod_j p_j^{t_j}$. We find that $t_i \leq n_{i,j}$ for all i, so $t_j \leq m_j$. Therefore, $d' \mid d$.

The argument for lcm is similar. ■

Lecture 15

22 Feb. 2022

2.5 Factorization in Polynomial Rings

Goal of today is to prove the following theorem.

Theorem 2.8. If R is a UFD, then $R[X]$ is a UFD.

In this section R is a UFD with field of fractions F. We have $R[X] \leq F[X]$. Moreover, $F[X]$ is a ED, hence a PID and UFD.

Definition 2.18. The *content* of $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ is $c(f) = \gcd(a_0, \ldots, a_n)$. (well-defined up to multiplication by a unit)

We say f is *primitive* if $c(f)$ is a unit.

Lemma 2.11.

1. If $f, g \in R[X]$ are primitive, then fg is primitive;
2. if $f, g \in R[X]$, then $c(fg) = c(f)c(g)$ (up to multiplication by a unit).

Proof.

1. Let $f = a_n X^n + \cdots + a_1 X + a_0$, $g = a_m X^m + \cdots + b_i X + b_0$. If fg is not primitive, $c(fg)$ is not a unit, so there is some prime p such that $p \mid c(fg)$.

   Since f, g are primitive, $p \nmid c(f)$ and $p \nmid c(g)$. Suppose $p \mid a_0, p \mid a_1, \ldots, p \nmid a_k$ and $p \mid b_0, p \mid b_1, \ldots, p \nmid b_l$. Then the coefficient of X^{k+l} in fg is

   $$\sum_{i+j=k+l} a_i b_j = \underbrace{\ldots + a_{k-1} b_{l+1}}_{\text{divisible by } p} + a_k b_l + \underbrace{a_{k+1} b_{l-1} + \ldots}_{\text{divisible by } p}.$$

   Thus, $p \mid a_k b_l \implies p \mid a_k$ or $p \mid b_l$ since p is prime.

2. Write $f = c(f) \cdot f_0$ and $g = c(g) \cdot g_0$ where f_0, g_0 are primitive polynomials. Then $fg = c(f)c(g)f_0 g_0$. So by the previous part, $c(fg) = c(f)c(g)$ (up to multiplication by unit).

■

Corollary 2.1. Let $p \in R$ be prime. Then p is prime in $R[X]$.

Proof. $R[X]^\times = R^\times$, so p is not a unit in $R[X]$.

Let $f \in R[X]$. Then $p \mid f$ in $R[X]$ if and only if $p \mid c(f)$ in R. Thus, if $p \mid gh$ in $R[X]$, we have $p \mid c(gh) = c(g)c(h)$. Because p is prime, we have $p \mid c(g)$ or $p \mid c(h)$. So, $p \mid g$ or $p \mid h$. That is, p is prime in $R[X]$. ■

Lemma 2.12. Let $f, g \in R[X]$ with g primitive. If $g \mid f$ in $F[X]$, then $g \mid f$ in $R[X]$.

Proof. Let $f = gh$ with $h \in F[X]$. Let $0 \neq a \in R$ such that $ah \in R[X]$, and write $ah = c(ah)h_0$ with h_0 primitive. Then $af = c(ah)h_0 g$ with $h_0 g$ primitive. Taking contents, we find $a \mid c(ah)$. Thus, $h \in R[X]$ and $g \mid f$ in $R[X]$. ■

Lemma 2.13 (Gauss's Lemma). Let $f \in R[X]$ be primitive. Then f irreducible in $R[X] \implies f$ irreducible in $F[X]$.

Proof. Since $f \in R[X]$ is irreducible and primitive, we have $\deg f > 0$, and so f is not a unit in $F[X]$.

Suppose that f is not irreducible in $F[X]$, say $f = gh$ where $g, h \in F[X]$ with $\deg g, \deg h > 0$.

Let $\lambda \in F^\times$ such that $\lambda^{-1} g \in R[X]$ is primitive. (e.g., let $0 \neq b \in R$ such that $bg \in R[X]$, then $bg = c(bg)g_0$ with g_0 primitive, so $\lambda = \frac{c(bg)}{b} \in R^\times$). Upon replacing g be $\lambda^{-1} g$ and h by λh, we may assume $g \in R[X]$ be primitive.

Then Lemma (2.12) implies $h \in R[X]$ and so $f = gh$ in $R[X]$, with $\deg g, \deg h > 0$ so f is not irreducible, and contradiction. ■

Remark. We'll see that the reverse implication also holds.

Lemma 2.14. Let $g \in R[X]$ be a primitive. Then g prime in $F[X] \implies g$ prime in $R[X]$.

Proof. Suppose $f_1, f_2 \in R[X]$ and $g \mid f_1 f_2$ in $R[X]$. Because g is prime in $F[X]$, $g \mid f_1$ or $g \mid f_2$ in $F[X]$. By Lemma (2.12), $g \mid f_1$ or $g \mid f_2$ in $R[X]$. That is, g is prime in $R[X]$. ■

Proof of Theorem (2.8). Let $f \in R[X]$. Write $f = c(f)f_0$ with $f_0 \in R[X]$ primitive. R is a UFD, so $c(f)$ is a product of irreducibles in R, which are also irreducible in $R[X]$.

If f_0 is not irreducible, say $f_0 = gh$, then $\deg g, \deg h > 0$ since f_0 is primitive, and g, h are also primitive. By induction on degree, f_0 is a product of irreducible in $R[X]$. This establishes (1) in definition of UFD.

By Proposition (2.7), suffices to show that if $f \in R[X]$ is irreducible then f is prime. Write $f = c(f)f_0$ with f_0 primitive. Since f is irreducible, then f is either constant or primitive.

When f is constant, f is irreducible in $R[X] \implies f$ is irreducible in $R \implies f$ prime in $R \implies f$ prime in $R[X]$ by Corollary (2.1).

When f is primitive, f irreducible in $R[X] \implies f$ is irreducible in $F[X]$ by Gauss's Lemma. Because $F[X]$ is a UFD, f is prime in $F[X] \implies f$ prime in $R[X]$ by Lemma (2.14). ■

Remark. By Lemma (2.8), the last three implications are actually if and only if.

Lecture 16

24 Feb. 2022

Example.

1. By Theorem (2.8), $\mathbb{Z}[X]$ is a UFD.
2. $R[X_1, \dots, X_n]$ be the polynomial ring in $X_1, \dots, X_n$ with coefficients in R. We can define it inductively by $R[X_1, \dots, X_n] = R[R_1, \dots, X_{n-1}][X_n]$. Applying Theorem (2.8) inductively, $R[X_1, \dots, X_n]$ is a UFD if R is a UFD.

Theorem 2.9 (Eisenstein's Criterion). Let R be a UFD and $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ primitive. Suppose $\exists p \in R$ irreducible such that

1. $p \nmid a_n$;
2. $p \mid a_i$ for all $0 \leq i \leq n-1$;
3. $p^2 \nmid a_0$.

Then f is irreducible in $R[X]$.

Proof. Suppose $f = gh$ with $g, h \in R[X]$ not units. f primitive implies that $\deg g, \deg h > 0$. Let $g = r_k X^k + \cdots + r_1 X + r_0$, and $h = s_l X^l + \cdots + s_1 X + s_0$ with $k + l = n$. Then $p \nmid a_n = r_k s_l \implies p \nmid r_k$ and $p \nmid s_l$, and $p \mid a_0 = r_0 s_0 \implies p \mid r_0$ or $p \mid s_0$. WLOG, $p \mid r_0$. Then $\exists j \leq k$ such that $p \mid r_0, p \mid r_1, \dots, r \mid r_{j-1}, r \nmid r_j$, and

$$a_j = r_0 s_j + r_1 s_{j-1} + \cdots + r_{j-1} s_1 + r_j s_0.$$

Since $j < n$, $p \mid a_j$, we have $p \mid r_j s_0 \implies p \mid s_0 \implies p^2 \mid r_0 s_0 = a_0$, ↯. ■

Example. 1. $f(X) = X^3 + 2X + 5 \in \mathbb{Z}[X]$.

If f is not irreducible in $\mathbb{Z}[X]$, then

$$f(X) = (X + a)(X^2 + bX + c)$$

with $a, b, c \in \mathbb{Z}$. Thus, $ac = 5$, but $\pm 1, \pm 5$ re not roots of f, contradiction.

By Gauss's Lemma, f is irreducible in $\mathbb{Q}[X]$. Thus, $\mathbb{Q}[X]/(f)$ is a field.

2. Let $p \in \mathbb{Z}$ prime. Eisenstein's Criterion tells us $X^n - p$ is irreducible in $\mathbb{Z}[X]$. Hence, it is irreducible in $\mathbb{Q}[X]$ by Gauss's Lemma.

3. Let $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ where $p \in \mathbb{Z}$ is a prime number. Eisenstein does not apply directly. But note that $f(X) = \frac{X^p - 1}{X - 1}$. Substituting $Y = X - 1$ gives

$$f(Y+1) = \frac{(Y+1)^p - 1}{(Y+1) - 1} = Y^{p-1} + \binom{p}{1} Y^{p-2} + \cdots + \binom{p}{p-2} Y + \binom{p}{p-1}.$$

Now $p \mid \binom{p}{i}$ for all $1 \leq i \leq p-1$ and $p^2 \nmid \binom{p}{p-1} = p$. Thus, $f(Y+1)$ is irreducible in $\mathbb{Z}[X]$, and $f(X)$ is irreducible in $\mathbb{Z}[X]$.

This gives the cyclotomic extension of the rationals.

2.6 Algebraic Integers

Recall $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$, the ring of Gaussian integers. The norm function $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ that maps $a+bi \mapsto a^2+b^2$ with $N(z_1 z_2) = N(z_1)N(z_2)$ is a Euclidean function. Thus, $\mathbb{Z}[i]$ is a ED, hence UFD and PID, and so primes are the same as irreducibles in $\mathbb{Z}[i]$.

The units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$ which are the only elements of norm 1.

Example. 1. $2 = (1+i)(1-i)$ and $5 = (2+i)(2-i)$ are not primes in $\mathbb{Z}[i]$.

2. $N(3) = 9$ so if $3 = ab$ in $\mathbb{Z}[i]$, $N(a)N(b) = 9$. But $\mathbb{Z}[i]$ has no elements of norm 3. Thus, either a or b is a unit, so 3 is irreducible, and hence prime.

   Similarly, 7 is prime in $\mathbb{Z}[i]$.

Proposition 2.9. Let $p \in \mathbb{Z}$ be a prime number. Then the following are equivalent.

1. p is not prime in $\mathbb{Z}[i]$.
2. $p = a^2 + b^2$ for some integers $a, b \in \mathbb{Z}$.
3. $p = 2$ or $p \equiv 1 \bmod 4$.

Proof. (1) $\implies$ (2). Let $p = xy$ where $x, y \in \mathbb{Z}[i]$ not units. Then $p^2 = N(p) = N(x)N(y)$, $N(x), N(y) > 1$. Thus, $N(x) = N(y) = y$. Writing $x = a + bi$ gives $p = N(x) = a^2 + b^2$.

(2) $\implies$ (3). The squares mod 4 are 0 and 1. Thus, if $p = a^2 + b^2$, then $p \not\equiv 3 \bmod 4$.

(3) $\implies$ (1). Already know that 2 is not prime in $\mathbb{Z}[i]$. We know $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic with order $p - 1$. So if $p \equiv 1 \bmod 4$, then $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element of order 4. That is, exists $x \in \mathbb{Z}$ with $x^4 \equiv 1 \bmod p$ but $x^2 \not\equiv 1 \bmod p$. Then $x^2 \equiv -1 \bmod p$. Now $p \mid x^2 + 1 = (x+i)(x-i)$. But $p \nmid x + i$ and $p \nmid x - i$. Thus, p is not prime in $\mathbb{Z}[i]$. ∎

Remark. We also proved (3) $\implies$ (2) in the process. It is an important result in number theory about sum of squares.

Theorem 2.10. The primes in $\mathbb{Z}[i]$ (up to associates) are

1. $a+bi$, where $a, b \in \mathbb{Z}$ and $a^2+b^2 = p$ is a prime number with $p = 2$ or $p \equiv 1 \bmod 4$;
2. prime numbers $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$.

Proof. We first prove that they are indeed prime.

1. $N(a+bi) = p$. If $a+bi = uv$, then either $N(u) = 1$ or $N(v) = 1$. Thus, $a+bi$ is irreducible and hence prime.
2. Proposition (2.9).

Now let $z \in \mathbb{Z}[i]$ be a prime (or irreducible). Then $\overline{z} \in \mathbb{Z}[i]$ is irreducible, and $N(z) = z\overline{z}$ is a factorization into irreducibles.

Let $p \in \mathbb{Z}$ be a prime such that $p \mid N(z)$ because $N(z) \neq 1$. If $p \equiv 3 \bmod 4$, then p is prime in $\mathbb{Z}[i]$. Thus, $p \mid z$ or $p \mid \overline{z}$, so p is an associate of z or $\overline{z}$. Consider the units in $\mathbb{Z}[i]$, we know p is an associate of z.

Otherwise, $p = 2$ or $p \equiv 1 \bmod 4$ and

$$p = a^2 + b^2 = (a+bi)(a-bi)$$

for some $a, b \in \mathbb{Z}$. Then

$$(a+bi)(a-bi) \mid z\overline{z}.$$

Thus, z is an associate of $a+bi$ or $a-bi$ by uniqueness of factorization. ∎

Lecture 17

26 Feb. 2022

Remark. In Theorem (2.10), if $p = a^2+b^2$, then $a+bi$ and $a-bi$ are not associates unless $p = 2$. $((1+i) = (1-i)i)$

Corollary 2.2. An integer $n \geq 1$ is the sum of 2 squares if and only if every prime factor p of n with $p \equiv 3 \bmod 4$ divides n to an even power.

Proof. $n = a^2+b^2$ if and only if $n = N(x)$ for some $x \in \mathbb{Z}[i]$ if and only if n is a product of norms of primes in $\mathbb{Z}[i]$. ∎