GRM

Lent 2016/2017

Contents

1 Groups

1.1 1.2

Definition. A homomorphism is called an *isomorphism* if it is a bijection. Say groups G and H are isomorphic if there exists an isomorphism $\phi : G \to H$ between them, write $G \cong H$.

Exercise: If ϕ is an isomorphism, then the inverse function $\phi^{-1} : H \to G$ is also a homomorphism (so an isomorphism).

Theorem. (First isomorphism theorem)
Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi) \triangleleft G$, $\operatorname{im}(\phi) \leq H$, and $G/\ker(\phi) \cong \operatorname{im}(\phi)$.

Proof. We've done the first two parts.
Let $f : G/\ker(\phi) \to \operatorname{im}(\phi)$ by $g\ker(\phi) \to \phi(g)$.
f is well-defined: if $g\ker(\phi) = g'\ker(\phi)$ then $g^{-1}g' \in \ker(\phi)$. So $e_H = \phi(g^{-1}g') = \phi(g^{-1}) \cdot \phi(g') = \phi(g)^{-1}\phi(g')$. So $\phi(g) = \phi(g')$. So we have $f(g\ker(\phi)) = f(g'\ker(\phi))$.

f is a homomorphism: $f(g\ker(\phi) \cdot g'\ker(\phi)) = f(gg'\ker(\phi)) = \phi(gg') = \phi(g)\phi(g') = f(g\ker(\phi)) \cdot f(g'\ker(\phi))$.

f is surjective: Let $h \in \operatorname{im}(\phi)$, i.e. $h = \phi(g)$ for some g. So $h = f(g\ker(\phi))$.

f is injective: Suppose $f(g\ker(\phi)) = e_H$, i.e. $\phi(g) = e_H$. Then $g \in \ker(\phi)$. So $g\ker(\phi) = e_G\ker(\phi)$. □

Example. Consider $\phi : \mathbb{C} \to \mathbb{C}\backslash\{0\}$ by $z \to e^z$. Then ϕ is a homomorphism from $(\mathbb{C}, +, 0)$ to $(\mathbb{C}\backslash\{0\}, \times, 1)$. ϕ is onto because log exists (principal value). We have

$$\ker(\phi) = \{z \in \mathbb{C} | e^z = 1\} = \{2\pi ik \in \mathbb{C} | k \in \mathbb{Z}\} = 2\pi i\mathbb{Z}$$

So from first isomorphism theorem we get $(\mathbb{C}/2\pi i\mathbb{Z}, +, 0) \cong (\mathbb{C}\backslash\{0\}, \times, 1)$.

Theorem. (Second isomorphism theorem)
Let $H \leq G$, $K \triangleleft G$. Then

$$HK = \{x = hk \in G | h \in H, k \in K\}$$

is a subgroup of G, $H \cap K \triangleleft H$, and

$$HK/K \cong H/H \cap K$$

Proof. Let $hk, h'k' \in HK$. Then

$$h'k'(hk)^{-1} = h'k'k^{-1}h^{-1} = h'h^{-1}hk'k^{-1}h^{-1}$$

$h'h^{-1} \in H$, and $hk'k^{-1}h^{-1} \in K$ since $K \triangleleft G$. So $h'k'(hk)^{-1} \in HK$. So $HK \leq G$.

Then consider $\phi : H \to G/K$ by $h \to hK$. This is a homomorphism (composition of $H \to G \to G/K$). Then

$$\ker(\phi) = \{h \in H | hK = eK\} = H \cap K$$

so $H \cap K$ is normal in H by first isomorphism theorem. Also

$$\text{im}(\phi) = \{gK \in G/K | gK = hK \text{ for some } h \in H\} = HK/K$$

So by first isomorphism theorem, $H/H \cap K \cong HK/K$ as required. □

Theorem. (Subgroup correspondence)
Let $K \lhd G$. There is a bijection between subgroups of G/K and subgroups of G that contain K by:
$\leftarrow$: $L/K \leq G/K \leftarrow K \lhd L \leq G$ and
$\rightarrow$: $U \leq G/K \rightarrow \{g \in G | gK \in U\}$.

The same maps give a bijection between normal subgroups of G/K and normal subgroups of G that contain K.

Theorem. (Third isomorphism theorem)
Let $K \lhd L$, $L \lhd G$. Then $(G/K)/(L/K) \cong G/L$.

Proof. Let $\phi : G/K \to G/L$ by $gK \to gL$.

ϕ is well-defined: if $gK = g'K$ then $g^{-1}g' \in K \leq L$. So $gL = g(g^{-1}g')L = g'L$.

ϕ is clearly surjective, and $\ker(\phi) = \{gK \in G/K | gL = eL \iff g \in L\} = L/K$.

So by first isomorphism theorem, $(G/K)/(L/K) \cong G/L$. □

Definition. A group G is *simple* if its only normal subgroups are $\{e\}$ and G.

Lemma. An abelian group is simple iff it is isomorphic to C_p for prime p.

Proof. In an abelian group, every subgroup is normal. Now let $g \in G$ be non-trivial and consider $H = \{..., g^{-1}, e, g, ...\}$. This is a subgroup of G, so a normal subgroup of G. If G is simple, then since g is non-trivial, this must be equal to G. So G is a cyclic group.

If G is infinite, then it is isomorphic to $(\mathbb{Z}, +, 0)$. But $2\mathbb{Z} \lhd \mathbb{Z}$. So this is not simple.

So $G \cong C_n$ for some n. If $n = a \cdot b$ for some $a, b \in \mathbb{Z}$ and $a, b \neq 1$, then G contains $< ..., g^{-a}, e, g^a, ... > \cong C_b$ as a proper subgroup. Contradiction.

So n must be a prime number.

Finally, note that C_p for prime p is indeed simple: by Lagrange theorem any subgroup of C_p must have order 1 or p. □

1.2 Actions and Permutations

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

Proof. We let G act on $X = G/H$, giving $\phi : G \to \text{Sym}(G/H)$. Then $\ker(\phi) \triangleleft G$, so as G is simple, either $\ker(\phi) = G$ or $\ker(\phi) = \{e\}$. But

$$\ker(\phi) = \bigcap_{g \in G} g^{-1}Hg \leq H$$

a proper subgroup of G; so the first case cannot occur. So $\ker(\phi) = \{e\}$.

By 1st isomorphism theorem,

$$G \cong G/\{e\} \cong \text{im}(\phi) = G^X \leq \text{Sym}(G/H) \cong S_n$$

Apply 2nd isomorphism theorem to $A_n \triangleleft S_n$, $G^X \leq S_n$. Then $G^X \cap A_n \triangleleft G^X$, $G^X/G^X \cap A_n = G^X A_n/A_n$. As $G^X \cong G$ is simple, $G^X \cap A_n \triangleleft G^X$, so $G^X \cap A_n = \{e\}$ or $G^X \cap A_n = \{e\}$. But if the first case holds, then $G^X \cong G^X A_n/A_n \leq S_n/A_n \cong C_2$, contradicting $G^X \cong G$ being non-abelian. Hence $G^X \cap A_n = G^X$, i.e. $G^X \leq A_n$.

$n \geq 5$ because A_2, A_3, A_4 have no non-abelian simple subgroups.

□

Corollary. If G is non-abelian simple, $H \leq G$ is of index n, then $|G| \mid \frac{n!}{2}$.

Definition. If G acts on X, the *orbit* of $x \in X$ is

$$G \cdot x = \{y = g * x \in X | g \in G\}$$

and the *stabiliser* of $x \in X$ is

$$G_x = \{g \in G | g * x = x\} \leq G.$$

Theorem. (Orbit-stabiliser).
If G acts on X, then for any $x \in X$, there is a bijection between $G \cdot x$ and G/G_x by $g * x \to gG_x$, $gG_x \leftarrow y = g * x$.

1.3 Conjugacy classes, centralisers and normalisers

There is an action of G on the set $X = G$ via $g * x := g \cdot x \cdot g^{-1}$.

This gives a map $\phi : G \to \text{Sym}(G)$. Note $\phi(g)(x \cdot t) = g \cdot x \cdot t \cdot g^{-1} = gxg^{-1}gtg^{-1} = \phi(g)(x) \cdot \phi(g)(t)$, i.e. $\phi(g)$ is a group homomorphism. Also it's a bijection (in $\text{Sym}(G)$), so it is an isomorphism.

Let $\text{Aut}(G) = \{f : G \to G | f \text{ is a group isomoprhism } \} \leq \text{Sym}(G)$, called the automorphisms of G.

We have shown that $\phi : G \to \text{Sym}(G)$ has image in $\text{Aut}(G) \leq \text{Sym}(G)$.

Definition. The *conjugacy class* of $x \in G$ is $G \cdot x = Cl_G(x) = \{gxg^{-1} | g \in G\}$.
The *centraliser* of $x \in G$ is $G_x = C_G(x) = \{g \in G | gxg^{-1} = x \iff gx = xg\}$.
The *centre* of G is $Z(G) = G_X = \ker(\phi) = \{g \in G | gxg^{-1} = x \forall x \in G\}$.
The *normaliser* of $H \leq G$ is $N_G(H) = \{g \in G | gHg^{-1} = H\}$.

By Orbit-stabiliser theorem, there is a bijection between $Cl_G(x)$ and $G/C_G(x)$. So if G is finite, then $|Cl_G(x)|$ equals the index of $C_G(x) \leq G$ which divides $|G|$.

Recall (from IA groups) that in S_n,
(i) everything can be written as a product of disjoint cycles;
(ii) permutations are conjugate iff they have the same cycle type.

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

Proof. First, claim A_n is generated by $3-$cycles.

Need to show that a product of two transposition is a product of $3-$cycles. We have $(ab)(bc) = (abc)$, $(ab)(cd) = (acb)(acd)$.

Let $H \triangleleft A_n$. *If* H contains a $3-$cycle, say (abc).

In S_n, there is a σ so that $(abc) = \sigma^{-1}(123)\sigma$. If $\sigma \in A_n$, then $(123) \in H$. Otherwise, let $\sigma' = (45)\sigma \in A_n$. Then $\sigma(123)\sigma = (abc)$.

So all $3-$cycles are in H if one of them is in H. In that case we know $H = A_n$.

So it is enough to show that any $\{e\} \neq H \triangleleft A_n$ contains a $3-$cycle.

Case 1: H contains $\sigma = (123...r)\tau$ in disjoint cycle notation for some $r \geq 4$. Let $\delta = (123)$ and consider $\sigma^{-1}\delta^{-1}\sigma\delta$. This is in H. Evaluate it and we get

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= \tau^{-1}(r...21)(132)(12...r)\tau(123)\\ &= (r...21)(132)(12...r)(123)\\ &= (23r) \in H\end{aligned}$$

is a $3-$cycle.

Case 2: H contains $\sigma = (123)(456)\tau$ in disjoint cycle notation. Let $\delta = (124)$ and calculate

$$\sigma^{-1}\delta^{-1}\sigma\delta = (132)(465)(142)(123)(456)(124) = (12436)$$

So we've reduced to the first case.

Case 3: H contains $\sigma = (123)\tau$, and τ is a product of $2-$cycles. Then $\sigma^2 = (132) \in H$.

Case 4: H contains $\sigma = (12)(34)\tau$, and τ is a product of $2-$cycles. Let $\delta = (123)$, then

$$u = \sigma^{-1}\delta^{-1}\sigma\delta = (12)(34)(132)(12)(34)(123) = (14)(23)$$

Now let $v = (152)u(125) = (13)(45)$. We have $u \cdot v = (14)(23)(13)(45) = (12345)$. So we've reduced to the first case.

So H contains a $3-$cycle.

□

1.4 p-groups

A finite group G is a p-group if $|G| = p^n$ for some prime number p.

Theorem. If G is a finite p-group, then $Z(G) \neq \{e\}$.

Proof. The conjugacy classes partition G, and

$$|Cl(x)| = |G/C_G(x)| \mid |G|$$

by Orbit-Stabilizer and Lagrange's Theorem. So $|Cl(x)|$ is a power of p.

We know $|G|$ is the sum of sizes of conjugacy classes. We can write $|G|$ = number of conjugacy classes of size 1 + size of all other conjugacy classes (which is divisible by p). Since $p \mid |G|$, the number of conjugacy classes of size 1 is divisible by p. In particular, $|Cl(e)| = 1$, so there is at least p of such conjugacy classes.

Now note that $Z(G)$ consider all the elements that commutes with all the elements in the group, i.e. they have conjugacy classes of size 1. So $|Z(G)| \geq p$. □

Corollary. A group of order p^n, $n > 1$, is *never* simple.

Lemma. For any group G, if $G/Z(G)$ is cyclic, then G is abelian.

Proof. Let the coset $gZ(G)$ generate the cyclic group $G/Z(G)$. Then every coset is a of the form $g^r Z(G)$, $r \in \mathbb{Z}$. So every element of G is of the form $g^r \cdot z$ for $z \in Z(G)$. Now take

$$(g^r z) \cdot (g^{r'} z') = g^r g^{r'} z z' = g^{r'} g^r z' z = g^{r'} z' g^r z$$

So G is abelian. □

Corollary. If $|G| = p^2$, p is prime, then G is abelian.

Proof. We know $\{e\} \lneq Z(G) \leq G$, so $|Z(G)| = p$ or p^2. If it's p^2 then $G = Z(G)$ is abelian.

If $|Z(G)| = p$, then $|G/Z(G)| = p$. So $G/Z(G)$ is cyclic. So G is abelian. □

Theorem. If $|G| = p^a$, then G has a subgroup of order p^b for any $0 \leq b \leq a$.

Proof. Prove by induction on a. If $a = 1$ then done. For $a > 1$, have $\{e\} \lneq Z(G)$. Let $e \neq x \in Z(G)$. Then x has order a power of p, so we can take some power of p that has order p, say z. Let $C = \langle z \rangle$, a normal subgroup of G (since this is inside centre). Now G/C has order p^{a-1}. By induction hypothesis, we may find a subgroup $H \leq G/C$ of order p^{b-1}. Now by subgroup correspondence, this H gives some $L \leq G$ that contains C (by $H = L/C$), and $|L| = p^b$. □

1.5 Finite abelian groups

Theorem. If G is a finite abelian group, then

$$G \cong C_{d_1} \times c_{d_2} \times ... \times C_{d_k}$$

with $d_{i+1}|d_i$ for all i.

We will prove this later, by considering an abelian group as a $\mathbb{Z}$-module.

Example. If $|G| = 8$ and G is abelian, then G is either C_8, or $C_4 \times C_2$, or $C_2 \times C_2 \times C_2$.

Lemma. (Chinese Remainder Theorem)
If n, m are coprime, then $C_{nm} \cong C_n \times C_m$.

Proof. Let $g \in C_n$ have order n, $h \in C_m$ has order m. Consider $x = (g, h)$ in $C_n \times C_m$. Clearly $x^{nm} = (e, e)$.

Now if $(e, e) = x^r = (g^r, h^r)$, then $n \mid r$ and $m \mid r$. So $nm \mid r$. So the order of x is nm. So $\langle x \rangle \cong C_{nm}$. Then by size we get the desired result. □

Corollary. If G is a finite abelian group, then

$$G \cong C_{n_1} \times C_{n_2} \times ... \times C_{n_l}$$

with each n_i a power of a prime number.

Proof. If $d = p_1 a^1 ... p_r a^r$ for distinct prime p_i, the lemma shows

$$C_d \cong C_{p_1 a^1} \times C_{p_2 a^2} \times ... \times C_{p_r a^r}$$

Apply this to the theorem. □

1.6 Sylow's Theorems

Theorem. (Sylow's)
Let $|G| = p^a \cdot m$, with $(p, m) = 1$, where p is prime. Then
(i) The set $Syl_p(G) = \{P \leq G \mid |P| = p^a\}$ of *Sylow p-subgroup* is not empty.
(ii) All elements inf $Syl_p(G)$ are conjugate in G.
(iii) The number $n_p = |Syl_p(G)|$ satisfies $n + p \equiv 1 \pmod p$ and $n_p \mid |G|$ (i.e. $n_p \mid m$).

Lemma. If $n_p = 1$, then the unique Sylow p-subgroup is normal in G.

Proof. If $g \in G$, $P \leq G$ the Sylow subgroup, then $g^{-1}Pg$ is a subgroup of order p^a. But P is the only such subgroup. □

Note that this tells that, if G is simple, then $n_p \neq 1$; or conversely, if $n_p = 1$ for some p, then G is not simple.

Example. Let $|G| = 96 = 2^5 \cdot 3$. So $n_2 \equiv 1 \pmod 2$ and $n_2 \mid 3$. So $n_2 = 1$ or 3. Also, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 32$. So $n_3 = 1, 4, 16$.

G acts on the set $Syl_p(G)$ by conjugation. So (ii) of the theorem says that this action has 1 orbit. The stabilizer of $P \in Syl_p(G)$, i.e. the normalizer $N_G(P) \leq G$, is of index $n_p = |Syl_p(G)|$.

Corollary. If G is non-abelian simple, then

$$|G| \mid \frac{(n_p)!}{2}.$$

and $n_p \geq 5$.

Proof. $N_G(P)$ has index n_p. So apply the general result about subgroups of non-abelian simple groups (see section 1.2). □

Now in the above example, $|G| \nmid \frac{3!}{2}$, so the group G cannot be non-abelian simple. Also it cannot be abelian simple as 96 is not a prime.

Example. Suppose G is a simple group of order $132 = 2^2 \times 3 \times 11$.

We know $n_{11} = 1 \pmod{11}$ and $n_{11}|12$. As G is simple we can't have $n_{11} = 1$, so $n_{11} = 12$.

Each Sylow 11-subgroup has order 11, so is isomorphic to C_{11}, so contains $10 = (11 - 1)$ elements of order 11. Such subgroups can only intersect in the identity element, so we have $12{+}10 = 120$ elements of order 11. We know $n_3 \equiv 1 \pmod 3$ and $n_3|44$, so $n_3 = 1, 4$ or 22 but similarly $n_3 \neq 1$. If $n_3 = 4$ then we need $|G| \mid \frac{4!}{2}|$ which is impossible. So $n_3 = 22$. But then by counting the number of elements we get a contradiction.

Proof of Sylow's Theorems. Let $|G| = p^n \cdot m$.
i) Let Ω be the set of subsets of G of order p^n, and let G act on Ω via $g * \{g_1, ..., g_{p^n}\} = \{gg_1, ..., gg_{p^n}\}$.
Let $\varepsilon \subset \Omega$ be an orbit for this action. If $\{g_1, ..., g_{p^n}\} = \varepsilon$, then

$$(gg_1^{-1}) * \{g_1, ..., g_{p^n}\} = \varepsilon = \{g, gg_1^{-1}g_2, ..., gg_1^{-1}g_{p^n}\}$$

So for any $g \in G$, there is an element of ε which contains g. So $|\varepsilon| \geq \frac{|G|}{p^n} = m$.

If there is some orbit ε with $|\varepsilon| = m$, then the stabilizer G_ε has order $\frac{|G|}{|\varepsilon|} = \frac{p^n m}{m} = p^n$, so G_ε *is* a Sylow $p-$subgroup. To show this happens, we must show that it is not possible for *every* orbit of G acting on Ω to have size $> m$.

By orbit-stabilizer, for any orbit ε, $|\varepsilon||p^n \cdot m$, so if $|\varepsilon| > m$, then $p||\varepsilon|$. So if *all* orbits of G acting on Ω has size $> m$, then p divides all of them, so $p||\Omega|$.

Let's calculate $|\Omega|$. We have

$$|\Omega| = \binom{p^n m}{p^n} = \prod_{j=0}^{p^n-1} \frac{p^n m ... j}{p^n ... j} (???)$$

The largest power of p dividing $p^n m = j$ is the same as the largest power of p dividing j, which is the same as the largest power of p dividing $p^n = j$. So $|\Omega|$ is *not* divisible by p.

ii)Let's show something *stronger*: if $p \in Syl_p(G)$ and Q is a $p-$subgroup, then there is a $g \in G$ s.t. $g^{-1}Qg \in P$.

Let G act on G/P by $q * g^p = qg^p$. By orbit-stabilizer, the size of an orbit divides $|Q| = p^n$, so is either 1 or divisible by p.

On the other hand, $|G/P| = \frac{|G|}{|P|} = m$ is not divisible by p. So ther must be an orbit of size 1, say $\{g^p\}$, i.e. for every $q \in Q$, $qg^p = g^p$ i.e. $g^{-1}qg \in P$ $\forall q \in Q$, i.e. $g^{-1}Qg \leq P$.

(iii) By (ii), G acts on $Syl_p(G)$ by conjugation with one orbit, so by orbit-stabilizer, $n_p \equiv |Syl_p(G)| \mid |G|$, which is the second part of (ii).

Example. Consider $GL_2(\mathbb{Z}/p)$. It has order $(p^2-1)(p^2-p) = p(p+1)(p-1)^2$. Let l be an odd prime dividing $p-1$ once only. Then $l \nmid p$. But also $l \nmid p+1$. So l^2 is the largest power of l dividing $|GL_2(\mathbb{Z}/p)|$, i.e. there is at least a subgroup of order l^2. We have

$$\begin{aligned}(\mathbb{Z}/p)^X &= \{x \in \mathbb{Z}/p | \exists g \in \mathbb{Z}/p \ s.t. \ xy = 1 \in \mathbb{Z}/p\} \\ &= \{x \in \mathbb{Z}/p | x \neq 0\}\end{aligned}$$

has size $p-1$. As a group under *multiplication*, $(\mathbb{Z}/p)^X \cong C_{p-1}$. So there is a subgroup $C_l \leq C_{p-1}$, i.e. we can find a $1 \neq x \in (\mathbb{Z}/p)^X$ so that $x^l = 1$.

Now let

$$\begin{aligned}H &= \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in (\mathbb{Z}/p)^X \text{ has order } l \right\} \cong C_l \times C_l \\ &\leq GL_2(\mathbb{Z}/p)\end{aligned}$$

is a Sylow $l-$subgroup (order l^2).

Example. Consider

$$SL_2(\mathbb{Z}/p) = \ker(\det : GL_2(\mathbb{Z}/p) \to (\mathbb{Z}_p)^X\}$$

The determinant homomorphism is onto, so $SL_2(\mathbb{Z}/p) \leq GL_2(\mathbb{Z}/p)$ has index $(p-1)$. So $|SL_2(\mathbb{Z}/p)| = (p-1)p(p+1)$.

Now consider

$$PSL_2(\mathbb{Z}/p) := SL_2(\mathbb{Z}/p) / \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p) \right\}$$

If $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \in SL_2(\mathbb{Z}/p)$ then $\lambda^2 = 1 \in (\mathbb{Z}/p)^X \cong C_{p-1}$. As long as $p \geq 3$, there are two such λ, $+1$ and -1. So $|PSL_2(\mathbb{Z}/p)| = \frac{1}{2}(p-1)p(p+1)$.

Let $(\mathbb{Z}/p)_\infty = \mathbb{Z}/p \cup \{\infty\}$. Then $PSL_2(\mathbb{Z}/p)$ acts on $(\mathbb{Z}/p)_\infty$ by Möbius maps:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * z := \frac{az+b}{cz+d}$$

with the usual convention that if $cz + d = 0$ then we get ∞.

Example. Let $p = 5$, then this action gives a homomorphism $\phi : PSL_2(\mathbb{Z}/p) \to \mathrm{Sym}\left((\mathbb{Z}/5)_\infty\right) \cong S_6$.

We have $|PSL_2(\mathbb{Z}/5)| = \frac{1}{2} \cdot 4 \cdot 5 \cdot 6 = 60$.

Claim. ϕ is injective.

Proof. If $\frac{az+b}{cz+d} = z \ \forall z \in (\mathbb{Z}/p)_\infty$, set $z = 0$ we get $b = 0$. Set $z = \infty$ we get $c = 0$. Set $z = 1$ we get $a = d$. So $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in PSL_2(\mathbb{Z}/p)$. □

Claim. ϕ lands in $A_6 \leq S_6$.

Proof. Consider the composition

$$\psi : PSL_2(\mathbb{Z}/5) \to \mathrm{Sym}((\mathbb{Z}/5)_\infty) \cong S_6 \to \{\pm 1\}$$

by ϕ and *sgn* respectively. We need to show that $\psi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = +1$.

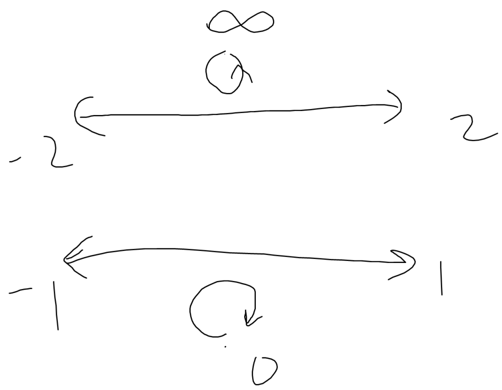
We know that elements of odd order in $PSL_2(\mathbb{Z}/5)$ have to be sent to $+1$.

Note that $H = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix}, \begin{bmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{bmatrix} \in PSL_2(\mathbb{Z}/5) \mid \lambda \in (\mathbb{Z}/5)^X \right\}$ has order 4 (note that λ and $-\lambda$ represent the same equivalence class as we are in PSL, so there are 2 of each kind), so is a Sylow 2−subgroup of $PSL_2(\mathbb{Z}/5)$. Any element of order 2 or 4 is conjugate to an element in H. We'll show that $\psi(H) = \{+1\}$.

H is generated by $\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Now consider

$$\begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$$

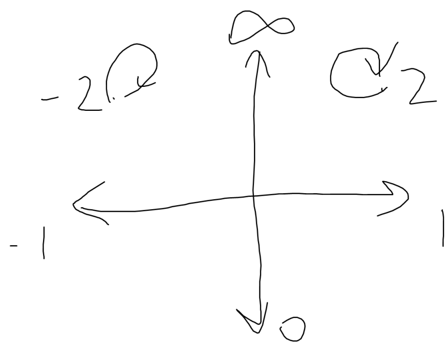
acting on $(\mathbb{Z}/5)_\infty$. This sends



so is an even permutation. Then

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

sends



is also even. So they are both in A_6.

□

2 Rings

In this course we only consider commutative rings with a multiplicative identity. Many of the things we are going to prove in this course will not hold without these two properties.

2.1 Definitions

Definition. A *ring* is a quintuple $(R, +, \cdot, 0_R, 1_R)$ s.t.
(R1) $(R, +, 0_R)$ is an abelian group;
(R2) The operation $- \cdot -\colon R \times R \to R$ is associative, and satisfies $1_R \cdot r = r = r \cdot 1_R$.
(R3) $r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2$, and $(r_1 + r_2) \cdot r = r_1 \cdot r + r_2 \cdot r$ (Distributivity).

A ring is *commutative* if in addition $a \cdot b = b \cdot a \ \forall a, b \in R$.

From now on every ring we discuss will by default be commutative and has a multiplicative identity.

Definition. If $(R, +, \cdot, 0_R, 1_R)$ is a ring ans $S \subset R$ is a subset, then it is called a *subring* if $0_R, 1_R \in S$ and $+, \cdot$ make S into a ring in its own right.

Example. We have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ as rings with the usual $0, 1, +, \cdot$.

Example. $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \leq \mathbb{C}$ is the subring called *Gaussian integers.*

Example. $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2} \cdot b \in \mathbb{R} \mid a, b \in \mathbb{Q}\} \leq \mathbb{R}$ is a subring.

Definition. An element $r \in R$ is a *unit* if there is a $s \in R$ s.t. $sr = 1_R$.

Note that this depends not only on the element but only on which ring we are talking about: $2 \in \mathbb{Z}$ is not a unit, but $2 \in \mathbb{Q}$ is.

If every $r \in R$ with $r \neq 0_R$ is a unit, then R is called a field.

Notation. If $x \in R$, write $-x \in R$ for the inverse of x in $(R, +, 0_R)$. We will write $y - x = y + (-x)$.

Example. $0_R + 0_R = 0_R$, so $r \cdot (0_R + 0_R) = r \cdot 0_R$, i.e. $r \cdot 0_R + r \cdot 0_R = r \cdot 0_R$, so $r \cdot 0_R = 0_R$. So if $R \neq \{0\}$, then $0_R \neq 1_R$, and 0_R is never a unit.

However, $(\{0\}, +, \cdot, 0, 0)$ *is* a valid ring.

Example. If R, S are rings, then $R \times S$ has the state of a ring via componentwise addition and multiplication, with $1 = (1_R, 1_S)$, $0 = (0_R, 0_S$.

Note that in this ring, $e_1 = (1_R, 0_S)$, $e_2 = (0_R, 1_S$, then $e_1^2 = e_1$ and $e_2^2 = e_2$, and $e_1 + e_2 = 1$.

Example. Let R be a ring. A *polynomial* f over R is an expression

$$f = a_0 + a_1 X + a_2 X^2 + ... + a_n X^n$$

with $a_i \in R$. X^i is just a symbol.

We will consider f and

$$a_0 + a_1X + ... + a_nX^n + 0_R \cdot X^{n+1}$$

as equal. The *degree* of f is the largest n s.t. $a_n \neq 0$.

If in addition, $a_n = 1_R$, then we say f is *monic*.

We write $R[X]$ for the set of all polynomials over R.

If $g = b_0 + ... + b_mX^m$, then we define addition and multiplication by the usual way:

$$f + g = \sum_{i=0}(a_i + b_i)X^i$$

$$f \cdot g = \sum_i \left(\sum_0^i a_j b_{i-j}\right) X^i$$

Now consider R as a subring of $R[X]$, given by the polynomials of degree 0. In particular, $1_R \in R$ gives the multiplicative identity element of $R[X]$.

Example. Write $R[[x]]$ for the ring of *formal power series*, i.e.

$$f = a_0 + a_1X + a_2X^2 + ...$$

with the same addition and multiplication.

Consider $\mathbb{Z}/2[X]$ and an element $f = X + X^2$. Then

$$f(0) = 0 + 0 = 0, f(1) = 1 + 1 = 0$$

But definitely $f \neq 0$. So we see the reason why we don't think f as functions despite that they do give functions. They are just elements in a particular ring.

Example. The *Laurent polynomials* $R[X, X^{-1}]$ is the set of

$$f = \sum_{i \in \mathbb{Z}} a_iX^i$$

s.t. only finitely many a_i are non-zero.

Example. The ring of *Laurent series* are those expressions

$$f = \sum_{i \in \mathbb{Z}} a_iX_i$$

with only finitely many $i < 0$ s.t. $a_i \neq 0$ (i.e. formal power series in the positive part and polynomial in the negative part). This is to make the sum in each coefficient a finite sum, as we didn't even define infinite sums in rings.

Example. If R is a ring and X is a set, the set R^X of all functions $f : X \to \mathbb{R}$ is a ring, with operations

$$(f + g)(X) = f(X) + g(X),$$
$$(fg)(X) = f(X) \cdot g(X).$$

The multiplicative identity element is the function $1(X) = 1_R$ for all X, and the same for the zero element.

Observe $\mathbb{R}^{\mathbb{R}} \supsetneq$ set of continuous $f : \mathbb{R} \to \mathbb{R} \supset$ polynomials $\mathbb{R} \to \mathbb{R} = \mathbb{R}[X]$. So $\mathbb{R}[X] \subsetneq \mathbb{R}^{\mathbb{R}}$.

2.2 Homomorphisms, ideals, quotients, and isomorphisms

Definition. A function $\phi : R \to S$ between rings is a *homomorphism* if
(H1) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$, i.e. ϕ is a group homomorphism between the additive groups of R and S;
(H2) $\phi(r_1 r_2)\phi(r_1)\phi(r_2)$;
(H3) $\phi(1_R) = 1_S$.

If in addition, ϕ is a bijection, then we say it is an *isomorphism.*

The *kernel* of $\phi : R \to S$ is

$$\ker(\phi) = \{r \in R | \phi(r) = 0\}$$

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

Proof. Note that $\phi : (R, +, 0_R) \to (S, +, 0_S)$ is a group homomorphism, and its kernel as a group homomorphism is also $\ker(\phi)$. So by theorems in groups we get the desired result. □

Definition. A subset $I \subset R$ is an *ideal*, written $I \triangleleft R$, if
(I1) I is a subgroup of $(R, +)$;
(I2) If $x \in I$, $r \in R$, then $x \cdot r \in I$ (strong multiplicative closure).

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

Lemma. If $\phi : R \to S$ is a homomorphism, then $\ker(\phi) \triangleleft R$.

Proof. (I1) holds for $\ker(\phi)$ since ϕ is a group homomorphism.

Now let $x \in \ker(\phi)$, $r \in R$. Then

$$\phi(r \cdot x) = \phi(r) \cdot \phi(x) = \phi(r) \cdot 0_S = 0_S$$

So $r \cdot x \in \ker(\phi)$. □

Example. If $I \triangleleft R$ and $1_R \in I$, then for any $r \in R$, we have

$$r = r \cdot 1 \in I,$$

so $I = R$. In short, proper ideals never include 1, so are never subrings.

Example. If R is a field, then $\{0\}$ and R are the only ideals. This is reversible: If $\{0\}$ and R are the only ideals, then R is a field.

Example. In the ring $\mathbb{Z}$, all ideals are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, where

$$n\mathbb{Z} = \{..., -2n, -n, 0, n, 2n, ...\}$$

Proof. $n\mathbb{Z}$ is certainly an ideal. Let $I \triangleleft \mathbb{Z}$ be an ideal. Let $n \in I$ be the smallest positive element. Then $n\mathbb{Z} \subset I$. If this is not an equality, choose $m \in I \backslash n\mathbb{Z}$. Then $m = n \cdot q + r$ for some $0 \leq r \leq n-1$. If $r = 0$ then $m \in I$, a contradiction. So

$$r = m - n \cdot q < n$$

is in the ideal I. Contradiction. □

Definition. For an element $a \in R$, write

$$(a) = \{a \cdot r | r \in R\}$$

the *ideal generated by a*. More generally, for a list $a_1, ..., a_s$, write

$$(a_1, ..., a_s) = \left\{ \sum_i a_i r_i | r_i \in R \right\}$$

which somewhat resembles the linear combinations in a vector space.

Even more generally, if $A \subseteq R$ is a subset, then the ideal generated by A is

$$(A) = \left\{ \sum_{a \in A} a \cdot r_a | r_a \in R, \text{only finitely many } r_a \neq 0 \right\}.$$

since we have no definition of infinite sums in rings.

If an ideal $I \triangleleft R$ is of the form (a), then we say that I is a *principal ideal.*

Example. In $\mathbb{Z}$ we have

$$n\mathbb{Z} = (n) \triangleleft \mathbb{Z}$$

is principal.

Example. In $\mathbb{C}[X]$, the polynomials with constant coefficient 0 forms an ideal, which is just (X) (check). This is also principal.

Proposition. Let $I \triangleleft R$ be an ideal. Define the *quotient ring* R/I to be the set of cosets $r + I$ (i.e. $(R, +, 0)$/normal subgroup I), with addition and multiplication given by

- $(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$,
- $(r_1 + I) + (r_2 + I) = r_1 r_2 + I$,

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

This is a ring, and the quotient map $R \to R/I$ by $r \to r + I$ is a ring homomorphism.

Proof. We already know that $(R/I, +, 0)$ is an abelian group. And addition as described above is well-defined. If $r_1 + I = r_1' + I$, $r_2 + I = r_2' + I$, then $r_1' - r_1 = a_1 \in I$, $r_2' - r_2 = a_2 \in I$. So

$$r_1' r_2' = (r_1 + a_1)(r_2 + a_2) = r_1 r_2 + r_1 a_2 + a_1 r_2 + a_1 a_2 = r_1 r_2 + a$$

for some $a \in I$, i.e. $r_1'r_2' + I = r_1r_2 + I$. So multiplication is well-defined. The ring axioms for R/I then follow from those of R. □

Example. $n\mathbb{Z} \lhd \mathbb{Z}$, so have a ring $\mathbb{Z}/n\mathbb{Z}$. This has elements $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}$, and addition and multiplication are modular arithmetic $(\text{mod } n)$.

Example. $(X) \lhd \mathbb{C}[X]$, so we have a ring $\mathbb{C}[X]/(X)$. Then

$$a_0 + a_1X + a_2X^2 + ... + a_nX^n + (X) = a_0 + (X).$$

If $a_0 + (X) = b_0 + (X)$, then $a_0 - b_0 \in (X)$. So $X | a_0 - b_0$, i.e. $a_0 = b_0$.

So consider

$$\begin{aligned} \phi : \mathbb{C}[X]/(X) \longleftarrow& \quad \mathbb{C} \\ a + (X) \longleftarrow& \quad a \end{aligned}$$

is surjective and injective. So ϕ is a bijection.

Observe that ϕ is a ring homomorphism. The inverse is $f + (X) \to f(0)$.

Proposition. (Euclidean algorithm for polynomials)
Let F be a field and $f, g \in F[X]$, then we may write

$$f = g \cdot q + r$$

with $\deg(r) < \deg(g)$.

Proof. Let
$\deg(f) = n$, so $f = a_0 + a_1X + ... + a_nX^n$ with $a_n \neq 0$;
$\deg(g) = m$, so $g = b_0 + b_1X + ... + b_mX^m$ with $b_m \neq 0$.

If $n < m$, let $q = 0$ and $r = f$.

Suppose $n \geq m$, and proceed by induction on n, Let

$$f_1 = f - g \cdot X^{n-m} \cdot a_n b_m^{-1}$$

we can do this because F is a field, so b_m has an inverse.

This has degree smaller than n.

If $n = m$, then $f = gX^{n-m}a_nb_m^{-1} + f_1$ where $\deg(f_1) < n = m$.

If $n > m$, by induction on degree, we have $f_1 = g \cdot q_1 + r$ with $\deg(r) < \deg(g)$.
So $f = gX^{n-m}a_n + b_m^{-1} + g \cdot q_1 + r = g(X^{n-m}b_m^{-1} + q_1) + r$ as required. □

Example. Consider $(X^2 + 1) \lhd \mathbb{R}[X]$, and $R = \mathbb{R}[X]/(X^2 + 1)$. Elements of R are of the form $f + (X^2 + 1)$. By Euclidean algorithm we have $f = q \cdot (X^2 + 1) + r$ with $\deg(r) < 2$. So $f + (X^2 + 1) = r + (X^2 + 1)$. So every coset is represented by a polynomial r of degree at most 1.

If $a_1 + b_1X + (X^2 + 1) = a_2 + b_2X + (X^2 + 1)$, then

$$X^2 + 1 | (a_1 + b_1X) - (a_2 + b_2X)$$

But by degree we know that $(a_1 + b_1X) - (a_2 + b_2X) = 0$. So take

$$\begin{aligned} \phi : \mathbb{R}[x]/(X^2+1) \to \mathbb{C} \\ a + bX + (X^2+1) \to a + bi \end{aligned}$$

This is a bijection. It sends addition to addition, and multiplication satisfies

$$\begin{aligned} &\phi((a + bX + (X^2+1)) \cdot (c + dX + (X^2+1))) \\ &= \phi(ac + (bc+ad)X + bdX^2 + (X^2+1)) \\ &= \phi(ac + (bc+ad)X + bd(-1) + bd(X^2+1) + (X^2+1)) \\ &= \phi((ac-bd) + (bc+ad)X + (X^2+1)) \\ &= (ac-bd) + (bc+ad)i \\ &= (a+ib)(c+id) \end{aligned}$$

So ϕ is a homomorphism. So $\mathbb{R}[x]/(X^2+1) \cong \mathbb{C}$.

We also have $\mathbb{Q}[x]/(X^2-2) = \mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$.

Theorem. (First isomorphism theorem)
Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi) \lhd R$, $\mathrm{im}(\phi) \leq S$, and $R/\ker(\phi) \cong \mathrm{im}(\phi)$ by $r + \ker(\phi) \to \phi(r)$.

Theorem. (Second isomorphism theorem)
Let $R \subset S$, $J \lhd S$. Then $R \cap J \lhd R$, $(R+J)/J = \{r + J | r \in R\} \leq S/J$, and $R/R \cap J = (R+J)/J$.

Theorem. (Subring correspondence)
We have a bijection between subrings of R/I and subrings of R containing I by:
$S/I \leq R/I \leftarrow I \lhd S \leq R$
$L \leq R/I \to \{r \in R | r + I \in L\}$, and the same map gievs a bijection between ideals of R/I and ideals of R containing I by

$$J/I \lhd R/I \leftrightarrow I \lhd J \lhd R.$$

Theorem. (Third isomorphism theorem)
Let $I, J \lhd R$, $I \subset J$. Then $J/I \lhd R/I$ and $(R/I)/(J/I) \cong R/J$.

Example. Consider the homomorphism $\phi : \mathbb{R}[X] \to \mathbb{C}$ by substituting in $X = i$, which is onto. We know

$$\ker(\phi) = \{f \in \mathbb{R}[x] | f(i) = 0\} = (X^2+1)$$

because real polynomials with i as a root also have $-i$ as a root. So are divisible by $(X-i)(X+i) = (X^2+1)$. Then by first isomorphism theorem,

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

(Compare with the previous proof).

Definition. For any ring R, there is a unique homomorphism

$$\begin{aligned} \iota : \mathbb{Z} &\to \mathbb{R} \\ 1 &\to 1_R \\ n > 0 &\to 1_R + 1_R + ... + 1_R \ (n \text{ times}) \\ n < 0 &\to -(1_R + 1_R + ... + 1_R) \ (-n \text{ times}) \end{aligned}$$

Note that $\ker(\iota) \lhd \mathbb{Z}$, so $\ker(i) = n\mathbb{Z}$ for some $n \geq 0$. This $n \geq 0$ is called the *characteristic* of the ring R.

Example. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ all have characteristic 0, while $\mathbb{Z}/n$ has characteristic n.

2.3 Integral domains, field of fractions, maximal and prime ideal

One thing to remember:

$$Field \implies ED \implies PID \implies UFD \implies ID.$$

The interesting bits start here.

Definition. A non-zero ring R is called an *integral domain (ID)* if for all $a, b \in R$, $a \cdot b = 0 \implies a = 0$ or $b = 0$.

We call x a *zero divisor* in R if $x \neq 0$ but $\exists y \neq 0$ s.t. $xy = 0$.

Example. All fields are integral domains. If $xy = 0$ with $y \neq 0$, then $xyy^{-1} = 0$ i.e. $x = 0$.

A subring of an integral domain is an integral domain, so $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Z}[i] \leq \mathbb{C}$ are integral domains.

Definition. A ring R is a *principal ideal domain (PID)* if it is an integral domain and every ideal is principal.

For example, $\mathbb{Z}$ is a principal ideal domain.

Lemma. A finite integral domain is a field.

Proof. Let $a \neq 0 \in R$, and consider

$$\begin{aligned} a \cdot - : R &\to R \\ b &\to ab \end{aligned}$$

This is a homomorphism of abelian groups and its kernel is $\{b \in R | ab = 0\} = \{0\}$. So $a \cdot -$ is injective. But R is finite. So $a \cdot -$ is bijective. In particular, $\exists b \in R$ s.t. $ab = 1$. So R is a field. □

Lemma. Let R be an integral domain, then $R[X]$ is also an integral domain.

Proof. Let $f = \sum_{i=0}^{n} a_i X^i$ and $a_n \neq 0$, $g = \sum_{i=0}^{m} b_i X^i$ and $b_m \neq 0$ be non-zero polynomials. Then the largest power of X in fg is X^{n+m} and its coefficient is $a_n b_m \neq 0$ as R is an ID. So $fg \neq 0$. □

Iterating this, we have

$$R[X_1, ..., X_n] = (((R[X_1])[X_2])...[X_n])$$

is an integral domain.

Theorem. Let R be an ID. There is a *field of fractions* F of R with the following properties:
(i) F is a field;
(ii) $R \leq F$;
(iii) every element of F is of the form $a \cdot b^{-1}$ for $a, b \leq R \leq F$.

Proof. Consider

$$S = \{(a, b) \in R \times R | b \neq 0\}$$

with the equivalence relation $(a, b) \sim (c, d) \iff ad = bc \in R$. This is reflexive and symmetric. For transitivity, if

$$(c, d) \sim (e, f)$$

Then $(ad)f = (bc)f = b(cf) = b(ed) \implies d(af - be) = 0$. But $d \neq 0$. So $af - be = 0$.

Let $F = S/\sim$. Write $[(a, b)] = \frac{a}{b}$ and define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd}.$$

and $0 = \frac{0}{1}$, $1 = \frac{1}{1}$.

If $\frac{a}{b} \neq 0$ then $a \cdot 1 \neq 0 \cdot b$, i.e. $a \neq 0$. Then $\frac{b}{a} \in F$, so $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$. So $\frac{a}{b}$ has an inverse, so F is a field.

We make $R \leq F$ by $\phi : R \to F$ by $r \to \frac{r}{1}$. □

Example. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$, and that of $\mathbb{C}[z]$ is the rational polynomial fractions in z.

Note: the ring $\{0\}$ is *not* afield.

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

Proof. If $I \triangleleft R$ is a non-zero ideal, then it contains $a \neq 0$. But an ideal containing a unit must be the whole ring. On the other hand, let $x \neq 0 \in R$, Then (x) must be R, as it is *not* the zero ideal. So $\exists y \in R$ s.t. $xy = 1_R$. So X is a unit. □

Definition. An ideal $I \triangleleft R$ is *maximal* if there is no proper ideal which properly contains I.

Lemma. An ideal I is maximal iff R/I is a field.

Proof. R/I is a field $\iff$ I/I and R/I are the only ideals in R/I $\iff$ $I, R\ triangleleft$ are the only ideals containing I by ideal correspondence. □

Definition. An ideal $I \triangleleft R$ is *prime* if I is proper, and if $a, b \in R$ are s.t. $a \cdot b \in I$, then $a \in I$ or $b \in I$.

Example. The ideal $n\mathbb{Z} \triangleleft \mathbb{Z}$ is prime if and only if n is zero and a prime number: if p is prime and $a \cdot b \in p\mathbb{Z}$, then $p|a \cdot b$, so $p|a$ or $p|b$, i.e. $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Conversely, if $n = uv$ is composite, $u \cdot v \in n\mathbb{Z}$ but $u, v \notin n\mathbb{Z}$.

Lemma. $I \triangleleft R$ is prime iff R/I is an integral domain.
Note that this shows that every maximal ideal is prime since fields are integral domains.

Proof. Suppose I is prime. Let $a + I, b + I \in R/I$ be s.t. $(a + I)(b + I) = 0$, i.e. $ab + I = 0$, so $ab \in I$. But I is prime, so $a \in I$ or $b \in I$. So $a + I = 0 + I$ or $b + I = 0 + I$ is the zero element in R/I. So R/I is an integral domain.

For the other direction, suppose R/I is an integral domain. Let $ab \in I$. Then $ab + I = 0$, so $(a + I)(b + I) = 0$. So $a + I = 0 + I$ or $b + I = 0 + I$, i.e. $a \in I$ or $b \in I$. □

Lemma. If R is an integral domain, then its characteristic is 0 or a prime number.

Proof. Let $\iota : \mathbb{Z} \to R$ with $1 \to 1_R$. Consider $\ker(\iota) = n\mathbb{Z}$. By 1st isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} \cong \text{im}(\phi) \leq R$ as a subring of an integral domain is again an integral domain, $Z/n\mathbb{Z}$ is an integral domain, so $n\mathbb{Z} \triangleleft \mathbb{Z}$ is prime. So n is zero or a prime number. □

2.4 Factorisation in integral domains

Suppose throughout this section that R is an integral domain.

Definition. 1) An element $a \in R$ is a unit if there is $b \in R$ s.t. $ab = 1$. Equivalently, $(a) = R$.
2) a divides b if there is $c \in R$ s.t. $b = a \cdot c$. Equivalently, $(b) \subset (a)$.
3) $a, b \in R$ are associates if $a = b \cdot c$ with c a unit. Equivalently, $(a) = (b)$, or $a|b$ and $b|a$.
4) $a \in R$ is irreducible if it is not 0, not a unit, and if $a = x \cdot y$ then x or y is a unit.
5) $a \in R$ is prime if it is not 0, not a unit, and when $a|x \cdot y$ then $a|x$ or $a|y$.

Note that $2 \in \mathbb{Z}$ is prime, but $2 \in \mathbb{Q}$ is not.
$2x \in \mathbb{Q}[x]$ is irreducible, $2x \in \mathbb{Z}[x]$ is not irreducible.

Lemma. (a) is a prime ideal in $R \iff r = 0$ or r is prime in R.

Proof. 1) let (r) be a prime, $r \neq 0$. As $(r) \neq R$, r is not a unit.
Suppose $r|a \cdot b$. Then $a \cdot b \in (r)$, but (r) is prime. So $a \in (r)$ or $b \in (r)$. So $r|a$ or $r|b$. So r is prime in R.
2) if $r = 0$ then (0) is a prime ideal since R is an integral domain.
Now let $r \neq 0$ and be prime in R.
Let $ab \in (r)$. Then $r|ab$. So $r|a$ or $r|b$. So $a \in (r)$ or $b \in (r)$. So (r) is a prime ideal in R. □

Lemma. if $r \in R$ is prime, then it is irreducible.

Proof. let $r \in R$ be prime, and suppose $r = a \cdot b$.
As r is prime, $r|a$ or $r|b$.
Suppose $r|a$. So $a = r \cdot c$. Then $r = r \cdot c \cdot b$.
As R is an integral domain,
$r(c \cdot b - 1) = 0 \implies c \cdot b = 1$.
So b is a unit. So r is irreducible. □

Example. Let $R = \mathbb{Z}[\sqrt{-5}] = \left\{a + b\sqrt{-5} | a \cdot b \in \mathbb{Z}\right\} \subseteq \mathbb{C}$.
$\mathbb{C}$ is a field and R is a subring, so R is an integral domain.
Consider the "norm":

$$\begin{aligned} N : R &\to \mathbb{Z} \geq 0 \\ a + b\sqrt{-5} &\to a^2 + 5b^2 \\ z &\to z\overline{z} = |z|^2. \end{aligned}$$

This satisfies $N(zw) = N(z) \cdot N(w)$.
If $r \cdot s = 1$ then $1 = N(1) = N(r \cdot s) = N(r) \cdot N(s)$.
So $N(s) = N(r) = 1$. So any unit has normal 1.
i.e. $a^2 + 5b^2 = 1$. Then $a = \pm 1, b = 0$: only $\pm 1 \in R$ are units.
Claim: $2 \in R$ is irreducible:
Suppose $2 = ab$. Then $4 = N(a) N(b)$.
Note that nothing in R has norm 2. So WLOG $N(a) = 1, N(b) = 4$. So a is a unit. So 2 is irreducible.
Similarly $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible (no r with $N(r) = 3$).
Note that $\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 6 = 2 \cdot 3$.
Claim: 2 does not divide $1 \pm \sqrt{-5} \implies 2$ is not prime:
if $2|1 + \sqrt{-5}$, then $N(2) | N\left(1 + \sqrt{-5}\right)$, i.e. $4|6$, contradiction.
Lessons: 1) irreducible doesn't imply prime in general.
2) $\left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right) = 2 \cdot 3$. So factorisation into irreducibles might not be unique.

Definition. an integral domain R is a *Euclidean domain*(ED) if there is a function $\varphi : R \backslash \{0\} \to \mathbb{Z} \geq 0$, a "Euclidean function", such that:
1) $\varphi(a \cdot b) \geq \varphi(b)$ for all $a, b \neq 0$;
2) if $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ s.t. $a = b \cdot q + r$, such that $r = 0$ or $\varphi(r) < \varphi(b)$ (r is "strictly smaller than" b).

Example. 1) $\mathbb{Z}$ is a Euclidean domain with $\varphi(n) = |n|$.
2) $F[x]$ with F a field is a Euclidean domain with $\varphi(f) = \deg(f)$.
3) $\mathbb{Z}[i] = R$ is Euclidean domain, with $\varphi(z) = N(z) = |z|^2 = z\overline{z}$:
i) $\varphi(zw) = \varphi(z)\varphi(w) \geq \varphi(z)$, as $\varphi(w) \in \mathbb{Z}^+$ for $w \neq 0$;

ii) let $a, b \in \mathbb{Z}[i]$. Consider $\frac{a}{b} \in \mathbb{C}$.
We know that $\exists q \in \mathbb{Z}[i]$ s.t. $|\frac{a}{b} - q| < 1$,i.e. $\frac{a}{b} = q + c$ with $|c| < 1$.
Then take $r = b \cdot c$, so $a = b \cdot q + b \cdot c = b \cdot q + r$.
$r = a - bq$, so r is in the ring $\mathbb{Z}[i]$; and $\varphi(r) = N(bc) = N(b) N(c) < N(b) = \varphi(b)$ since $N(c) < 1$.

Proposition. (ED $\implies$ PID)
if R is a Euclidean domain, then it is a principal ideal domain.

Proof. Let R have Euclidean function $\varphi : R \backslash \{0\} \to \mathbb{Z} \geq 0$. Let $I \triangleleft R$ be non-zero.
Let $b \in I \backslash \{0\}$ be an element with $\varphi(b)$ minimal.
Then for $a \in I$, write $a = bq + r$ with $r = 0$, or $\varphi(r) < \varphi(b)$. But $r = a - bq \in I$, so we can't have $\varphi(r) < \varphi(b)$. So $r = 0$.
Thus $a \in (b)$. Since a is arbitrary, $I \subset (b)$. But $(b) \in I$ as well, so $I = (b)$. So R is a principal ideal domain. □

Example. $\mathbb{Z}$,$F[X]$(F field) are Principal ideal domains.
$\mathbb{Z}[i]$ is a PID. In $\mathbb{Z}[X]$, $(2, x) \triangleleft \mathbb{Z}[X]$ is not a principal ideal.
Otherwise suppose $(2, x) = (f)$, then $2 = f \cdot g$ for some g. Then f has to have degree zero, so a constant, so $f \pm 1 or \pm 2$.
If $f = \pm 1$ a unit, then $(f) = \mathbb{Z}[x]$, but $1 \notin (2, x)$. Contradiction. If $f = \pm 2$, $x \in (2, x) = (f)$ so $\pm 2 | x$, a contradiction.

Example. Let $A \in M_{n \times n}(F)$ be an $n \times n$ matrix over a field F.
$I = \{f \in F[X] | f(A) = 0\}$.
If $f \cdot g \in I$,$(f + g)(A) = f(A) + g(A) = 0 + 0 = 0$.
If $f \in I, g \in F[X]$ then $(f \cdot g)(A) = f(A) \cdot g(A) = 0$
So I is an ideal.
So $F[X]$ is a PID, have $I = (m)$ for some $m \in F[X]$.
Suppose $f \in F[X]$ s.t. $f(A) = 0$. Then $f \in I$ so $f = m \cdot g$. So m is the minimal polynomial of A.

Definition. An integral domain is a unique factorization domain (UFD) if:
1) every non-unit may be written as a product of irreducible elements;
2) if $p_1 p_2 ... p_n = q_1 q_2 ... q_m$ with p_i, q_i irreducible, then $n = m$, and they can be reordered such that p_i is an associate of q_i. (they generate the same ideal)

Goal: want to show that PID $\implies$ UFD.

Lemma. Let R be a PID. If $p \in R$ is irreducible, then it is prime.
(prime $\implies$ irreducible in any integral domain)

Proof. Let $p \in R$ be irreducible. Suppose $p | a \cdot b$. Suppose $p \nmid a$.
Consider the ideal $(p, a) \triangleleft R$, a PID so $(p, a) = (d)$ for some $d \in \mathbb{R}$.
So $d | p$,so $p = q_1 \cdot d$ for some q_1.
We must have q_1 a unit or d a unit.
If q_1 a unit then $d = q_1^{-1} \cdot p$ divides a. So $a = q_1 \cdot p \cdot x$, contradiction.
Thus d is a unit, so $(p, a) = (d) = R$.

So we have $1_R = v \cdot p + s \cdot a$ for some $r, s \in R$.
So $b = r \cdot p \cdot b + s \cdot a \cdot b$. So $p|b$. □

Lemma. Let R be a PID, let $I_1 \in I_2 \in ...$ be a chain of ideals. Then there is a $N \in \mathbb{N}$ s.t. $I_n = I_{n+1} \forall n \geq \mathbb{N}$.(this is called the ascending chain condition(ACC), a ring satisfying this condition is called *Noetherian.*)

Proof. Let $I = \cup_{n\geq 1}^{\infty} I_n$, again an ideal. As R is a PID, $I = (a)$ for some $a \in R$.
This $a \in I = \cup_{n=0}^{\infty} I_n$, so $a \in I_n$ for some n.
Thus $(a) \leq I_n \leq I = (a)$.
So they are all equal. So $I_n = (a) = I$, so $I_n = I_N \forall n \geq N$. □

Proposition. PID $\implies$ UFD.

Proof. 1) Need to show any $r \in R$ is a product of irreducibles.
Let $r \in R$. If r is irreducible then we are done.
Suppose not, then $r = r_1 s_1$ with r_1, s_1 both non-units.
If both r_1, s_1 are reducible then we are done. Suppose not, WLOG write $r_1 = r_2 s_2$ with r_2, s_2 non-units.
Continue in this way. If the process doesn't end, $(r) \leq (r_1) \leq ... \leq (r_n) \leq ....$
So by the ACC property, $(r_n) = (r_{n+1}) = ...$ for some n.
So $r_n = r_{n+1} \cdot s_{n+1}$, and $(r_n) = (r_{n+1}) \implies s_{n+1}$ is a unit. Contradiction.
2) Let $p_1 p_2 ... p_n = q_1 q_2 ... q_n$ with p_i, q_i irreducible.
So $p_1 | q_1 ... q_n$. In a PID, irreducible $\iff$ prime. So p_1 divides some q_i, reorder to suppose $p_1 | q_1$. So $q_1 = p_1 \cdot a$. But as q_1 is irreducible, a must be a unit. So $p_1 and q_1$ are associates.
Cancelling p_1 gives:
$p_2 p_3 ... p_n = (a q_2) q_3 ... q_n$ and we continue.
This also shows $n = m$, else if $n = m + k$ then get $p_{k+1} ... p_n = 1$ a contradiction. □

Definition. d is a greatest common divisor of $a_1, a_2, ..., a_n$ if $d|a_i$ for all i, and if $d'|a_i$ for all i then $d'|d$.

Lemma. If R is a UFD then the gcd exists, and is unique up to associates.

Proof. Every a is a product of irreducibles, so let $p_1, p_2, ..., p_m$ be a list of all the irredcibles which are factors of a_i, none of them is associate of each other.
Write $a_i = u_i \Pi_{j=1}^{m} p_j^{n_{ij}}$ for u_i units and $n_{ij} \in \mathbb{N}$.
Let $m)j = \min_i (n_{ij})$ and $d = \Pi_{j=1}^{m} p_j^{m_j}$. As $m_j \leq n_{ij} \forall i$, $d|a_i$ for all i.
If $d'|a_i \forall i$, let $d' = v \Pi_{j=1}^{m} p_i^{t_j}$.
Then we must have $t_j \leq n_{ij} \forall i$ so $t_j \leq m_j \forall j$. Then $d'|d$. □

2.5 Factorisation in polynomial rings

For F a field, we know $F[x]$ is a Euclidean Domain(ED), so a PID, so a UFD. So
1) $I \triangleleft F[x] \implies I = (f)$.

2) $f \in F[x]$ irreducible $\iff$ f prime.
3) Let $f \in F[x]$ be irreducible, and $(f) \leq J \leq F[x]$. Then $J = (g)$ and $(f) \subset (g)$ so $f = g \cdot h$. But f is irreducible, so g or h is a unit.
If g is a unit, then $(g) = F[x]$;
If h is a unit, then $(f) = (g)$.
So (f) is a maximal ideal.
4) (f) prime ideal $\implies$ f prime $implies f$ reducible $\implies$ (f) is maximal.
So in $F[x]$, prime ideals are the same as maximal ideals.
5) f is irreducible if and only if $F[x]/(f)$ is a field.

Definition. Let R be a UFD and $f = a_0 + a_1X + ... + a_nX^n \in R[x]$ with $a_n \neq 0$. Let the *content* $c(f)$ of f is the gcd of all the coefficients in R, unique up to associates. Say f is *primitive* if $c(f)$ is a unit, i.e. the a_i are coprime.

Lemma. (Gauss') Let R be a UFD, $f \in R[x]$ be a primitive polynomial. Then f is irreducible in $R[x]$ $\iff$ f is irreducible in $F[x]$, where F is the field of fractions of R.

Example. Consider $f = x^3 + x + 1 \in \mathbb{Z}[x]$. This has content 1 so is primitive. Suppose f is reducible in $\mathbb{Q}[x]$. Then by Gauss' lemma f is reducible in $\mathbb{Z}[x]$ too, so $x^3 + x + 1 = g \cdot h$ for $g, h \in \mathbb{Z}[x]$, both g and h are not units. Neither g nor h can be constant, so they both have degree at least 1. So WLOG suppose g has degree 1 and h as degree 2.
So $g = b_0 + b_1x$, $h = c_0 + c_1x + c_1x^2$.
Multiplying them gives $b_0c_0 = 1$, $c_2b_1 = 1$ so b_0 and b_1 are both ± 1. So g is $1 + x$ or $1 - x$ or $-1 + x$ or $-1 - x$, so has ± 1 as a root. But f doesn't have ± 1 as a root. Contradiction.
Note that from this we can know that f has not no root in $\mathbb{Q}$.

Lemma. Let R be a UFD. If $f, g \in R[x]$ are primitive, then $f \cdot g$ is primitive too (Note that we don't know whether $R[x]$ is a UFD or not).

Proof. Let $f = a_0 + a_1x + ... + a_nx^n$ with $a_n \neq 0$,
$g = b_0 + b_1x + ... + b_mx^m$ with $b_m \neq 0$ be both primitive.
Suppose $f \cdot g$ is not primitive. Then $c(fg)$ is not a unit, so let p be an irreducible which divides $c(fg)$.
By assumption $c(f)$ and $c(g)$ are units, so $p \nmid c(f)$ and $p \nmid c(g)$.
Suppose $p|a_0$, $p|a_1$, ..., $p|a_{k-1}$, but $p \nmid a_k$;
$p|b_0$,...,$p|b_{l-1}$,but $p \nmid b_l$.
Look at coefficient of x^{k+l} in $f \cdot g$:
$... + a_{k+1}b_{l-1} + a_kb_l + a_{k-1}b_{l+1} + ... = \sum_{i+j=k+l} a_ib_j$.
As $p|c(fg)$, we have $p|\sum_{i+j=k+l} a_ib_j$.
We see that the only term that might not be divisible by p is a_kb_l.
So $p|a_kb_l$. p is irreducible (so prime), so $p|a_n$ or $p_b|l$. Contradiction.
So $f \cdot g$ is primitive. □

Corollary. let R be a UFD. Then for $f, g \in R[x]$ we have that $c(f \cdot g)$ is an associate of $c(f)\,c(g)$.

Proof. We can always write $f = c(f) f_1, g = c(g) g_1$ with f_1, g_1 being primitive. Then $f \cdot g = c(f) c(g)(f_1 \cdot g_1)$. So $c(f) c(g)$ is a gcd of coefficients $f \cdot g$, so is $c(fg)$ (up to associates). □

Proof. (Gauss' lemma)
We will show that a primitive $f \in R[x]$ is reducible in $R[x] \iff$ it is reducible in $F[x]$.
1) Let $f = g \cdot h$ be a product in $R[x]$, g, h not units. As f is primitive, so are g and h. So both have degree at least 1.
So g, h are not units in $F[x]$ either, so f is reducible in $F[x]$.
2) Let $f = g \cdot h$ in $F[x]$, g and h not units. So g and h have degree at least 1.
We can find $a, b \in R$ s.t. $a \cdot g \in R[x]$ and $b \cdot h \in R[x]$ (clear the denominators).
Then $a \cdot b \cdot f = (a \cdot g)(b \cdot h)$ is a factorisation in $R[x]$.
Let $(a \cdot g) = c(a \cdot g) \cdot g_1$ with g_1 primitive, $(b \cdot h) = c(b \cdot h) \cdot h_1$ with h_1 primitive.
So

$$\begin{aligned} a \cdot b &= c(a \cdot b \cdot f) \\ &= c((a \cdot g)(b \cdot h)) \\ &= u \cdot c(a \cdot g) \cdot c(b \cdot h) \end{aligned}$$

by the previous corollary, where $u \in R$ is a unit.
But also $a \cdot b \cdot f = c(a \cdot g) \cdot c(b \cdot h) \cdot g_1 \cdot h_1$.
So cancelling $a \cdot b$ gives $f = u^{-1} g_1 h_1 \in R[x]$, so f is reducible in $R[x]$. □

Proposition. Let R be a UFD, $g \in R[x]$ be primitive.
Let $J = (g) \lhd R[x]$, $I = (g) \lhd F[x]$.
Then $J = I \cap R[x]$.
(More plainly, if $f = g \cdot h \in R[x]$ with $h \in F[x]$ then $f = g \cdot h'$ with $h' \in R[x]$.

Proof. Certainly $J \subseteq I \cap R[x]$. Let $f \in I \cap R[x]$, so $f = g \cdot h$ with $h \in F[x]$.
Choose $b \in R$ s.t. $b \cdot h \in R[x]$ (clear denominators).
Then $b \cdot f = g \cdot (bh) \in R[x]$.
Let $(b \cdot h) = c(b \cdot h) \cdot h_1$ for h_1 primitive. Then
$b \cdot f = c(b \cdot h) \cdot g \cdot h_1$. So $c(bf) = u \cdot c(bh)$ for u a unit since $g \cdot h_1$ is primitive.
But $c(b \cdot f) = b \cdot c(f)$. So $b | c(bh)$.
$c(bh) = b \cdot c \in R$.
So $b \cdot f = b \cdot cgh_1$, cancelling b gives $f = g(ch_1)$. So g divides f in $R[x]$. □

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

Proof. Let $f \in R[x]$. We can write $f = c(f) \cdot f_1$ with f_1 primitive.
Firstly, As R is a UFD, we may factor $c(f) = p_1 p_2 ... p_n$ for $p_i \in R$ irreducible, (so also irreducible in $R[x]$).
If f_1 is not irreducible, write $f_1 = f_2 f_3$ with f_2 and f_3 both not units, so f_2 and f_3 must both have non-zero degree(since f_1 is primitive, they can't be constant).
Also $\deg(f_2), \deg(f_3) < \deg(f_1)$.
If f_2, f_3 are irreducible then done. Else continue factoring. At each stage the degree of factors strictly decreases, so we must finish: $f_1 = q_1 q_2 ... q_m$ with q_i irreducible.
So $f = p_1 p_2 ... p_n q_1 q_2 ... q_m$ is a product of irreducibles.

For uniqueness, first note that $c(f) = p_1 p_2 ... p_n$ is a unique factorisation up to reordering and associates, as R is a UFD. So cancel this off to obtain $f_1 = q_1...q_m$.So suppose $q_1 q_2 ... q_m = r_1 r_2 ... r_l$ is another factorisation of f_1.
Note that each q_i and each r_i is a factor of the primitive polynomial f_1, so each of them must be also primitive.
Let F be the field of fractions of R, and consider $q_i, r_i \in F[x]$ instead. Now $F[x]$ is a ED, hence PID, hence UFD. By Gauss' lemma, the q_i and r_i are irreducible in $F[x]$. As $F[x]$ is a UFD we find that $l = m$; and after reordering $r_i = u_i q_i$ with $u_i \in F[x]$ a unit.
Firstly $u_i \in F$ since it is a unit.
Clear denominators of u_i, we find that $a_i r_i = b_i q_i \in R[x]$.
So taking contents shows that a_i and b_i are associates. So $b_i = v_i a_i$ with $v_i \in R$ a unit.
Cancelling a_i gives $r_i = v_i q_i$ as required. □

Example. $\mathbb{Z}[x]$ is a UFD.
R is a UFD $\implies R[x_1, x_2, ..., x_n]$ is a UFD.

Theorem. (Eisenstein's criterion) Let R be a UFD, let

$$f = a_0 + a_1 x + ... + a_n x^n \in R[x]$$

have $a_n \neq 0$ and f primitive. Let $p \in R$ be irreducible (=prime, since R is a UFD) such that:
1) $p \nmid a_n$;
2) $p | a_i$ for $0 \le i \le n-1$;
3) $p^2 \nmid a_0$.
Then f is irreducible in $R[x]$, so also irreducible in $F[x]$ by Gauss' lemma.

Proof. Suppose f=$g \cdot h$ with
$g = r_0 + r_1 x + ... + r_k x^k$ with $r_k \neq 0$,
$h = s_0 + s_1 x + ... + s_l x^l$ with $s_l \neq 0$.
Now $r_k s_l = a_n$, and $p \nmid a_n$ so $p \nmid r_k$ and $p \nmid s_l$.
Also $r_0 s_0 = a_0$, and $p | a_0$ but $p^2 \nmid a_0$. So WLOG let $p | r_0$ but $p \nmid s_0$.
Let j be such that $p | r_0, p | r_1, ..., p | r_{j-1}, p \nmid r_j$.
Then $a_j = r_0 s_j + r_1 s_{j-1} + ... + r_{j-1} s_1 + r_j s_0$. All but the last term are divisible by p, and $r_j s_0$ is not divisible by p since both r_j and s_0 are not divisible by p.
So $p \nmid a_j$. By condition (1) and (2) we must have $j = n$. Also we have $j \le k \le n$, so $j = k = n$. That means $l = n - k = 0$, so h is a constant.
But f is primitive, it follows that h must be a unit. So f is irreducible. □

Example. Consider $x^n - p \in \mathbb{Z}[x]$ for p prime. Apply Eisenstein's criterion with p, we find that all the conditions hold. So $x^n - p$ is irreducible in $\mathbb{Z}[x]$, and so in $\mathbb{Q}[x]$ as well by Gauss' lemma.
This implies that $x^n - p$ has no roots in $\mathbb{Q}$. So $\sqrt[n]{p} \notin \mathbb{Q}$.

Example. Consider $f = x^{p-1} + x^{p-2} + ... + x^2 + x + 1 \in \mathbb{Z}[x]$ with p a prime number.
Note $f = \frac{x^p - 1}{x - 1}$, so let $y = x - 1$. Then
$\hat{f}(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + ... + \binom{p}{p-1}$.
Now $p | \binom{p}{i}$ for $1 \le i \le p-1$, but $p^2 \nmid \binom{p}{p-1} = p$.

So by Eisenstein's criterion, $\hat{f}$ is irreducible in $\mathbb{Z}[x]$.
Now if $f(x) = g(x) \cdot h(x) \in \mathbb{Z}[x]$, then get $\hat{f}(y) = g(y+1) \cdot h(y+1)$ a factorisation in $\mathbb{Z}[y]$. So f is irreducible.

2.6 Gaussian integers

Recall $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \leq \mathbb{C}$ is thexswq *Gaussian integers*.
The *norm* $N(a+ib) = a^2 + b^2$ serves as a Euclidean function for $\mathbb{Z}[i]$. So it is a ED, so a PID, so a UFD.
The units are precisely ± 1 and $\pm i$.

Example. 1) $2 = (1+i)(1-i)$, so not irreducible, so not prime.
2) 3: $N(3) = 9$, so if $3 = u \cdot v$ with u, v not units, then $9 = N(u) N(v)$ with $N(u) \neq 1 \neq N(v)$. So $N(u) = N(v) = 3$. But $3 = u^2 + v^2$ has no solutions with $a, b \in \mathbb{Z}$. So 3 is irreducible, so a prime.
3) $5 = (1+2i)(1-2i)$ is not irreducible, so not prime.

Proposition. A prime number $p \in \mathbb{Z}$ is prime in $\mathbb{Z}[i] \iff p \neq a^2 + b^2$ for $a, b \in \mathbb{Z} \setminus \{0\}$.

Proof. If $p = a^2 + b^2 = (a+ib)(a-ib)$ then it is not irreducible, so not prime.
If $p = u \cdot v$, then $p^2 = N(u) N(v)$. So if u, v are not units, then $N(u) = N(v) = p$ since p is prime in $\mathbb{Z}$. Writing $u = a + ib$, this says $a^2 + b^2 = p$. □

Lemma. Let p be a prime number, $F_p = \mathbb{Z}/p\mathbb{Z}$ a field with p elements.
Let $F_p^* = F_p \setminus \{0\}$ be the group of invertible elements under multiplication.
Then $F_p^* \cong C_{p-1}$.

Proof. Certainly F_p^* has order $p-1$, and is abelian.
Know classification of finite abelian groups, it follows that if F_p^* is not cyclic, then it must contain a subgroup $C_m \times C_m$ for $m > 1$.
Consider the polynomial $X^m - 1 \in F_p[x]$, a UFD. At best this factors into m linear factors, so $X^m - 1$ has at most m distinct roots.
If $C_m \times C_m \leq F_p^*$, then we have m^2 elements of F_p which are roots of $X^m - 1$.
But $m^2 > m$, contradiction. So F_p^* is cyclic. □

Proposition. The primes in $\mathbb{Z}[i]$ are, up to associates,
1) prime numbers $p \leq \mathbb{Z} \leq \mathbb{Z}[i]$ s.t. $p \equiv 3 \mod 4$;
2) $z \in \mathbb{Z}[i]$ with $N(z) = z\bar{z} = p$ for p prime, $p = 2$ or $p \equiv 1 \mod 4$.

Proof. 1) If $p \equiv 3 \mod 4$ then $p \neq a^2 + b^2$.
By the previous proposition, $p \in \mathbb{Z}[i]$ is prime.
2) If $N(z) = p$ and $z = uv$, then $N(u) N(v) = p$. So $N(u) = 1$ or $N(v) = 1$, so u or v is a unit.
Let $z \in \mathbb{Z}[i]$ be irreducible (also prime). Then $\bar{z}$ is irreducible, so $N(z) = z\bar{z}$ is a factorisation of $N(z)$ into irreducibles.
Let $p \in \mathbb{Z}$ be a prime number dividing $N(z)$. ($N(z) \neq 1$ so such p exists).

• Case 1: $p \equiv 3 \mod 4$. Then $p \in \mathbb{Z}[i]$ is prime by the first part of the proof. $p|N(z) = z\bar{z}$ so $p|z$ or $p|\bar{z}$. So perhaps conjugating, get $p|z$. But both are irreducible, so p and z are associates.
• Case 2: $p = 2$ or $p \equiv 1 \mod 4$.
If $p \equiv 1 \mod 4$ then $p - 1 = 4k$ for some k. As $F_p^* \cong C_{p-1} = C_{4k}$, there is a unique element of order 2, which must be $[-1] \in F_p$.
Let $[a] \in F_p^*$ be an element of order 4. Then $[a^2] = [-1]$.
So $a^2 + 1$ is divisible by p. So $p|(a+i)(a-i)$.
Also $2|(1+i)(1-i)$.
So deduce that p (or 2) is not prime, so not irreducible, as it clearly does not divide $a + i$ or $a - i$.
So $p = z_1 z_2$ for $z_1, z_2 \in \mathbb{Z}[i]$. So

$$p^2 = N(p) = N(z_1)N(z_2).$$

So as z_i are not units, $N(z_1) = N(z_2) = p$. So $p = z_1\bar{z_2}$ $(= z_2\bar{z_1})$. So $\bar{z_1} = z_2$. So $p = z_1\bar{z_1}|N(z) = z\bar{z}$. So z is an associate of z_1 or $\bar{z_1}$, as z and z_1 are irreducible. □

Corollary. An integer $n \in \mathbb{Z}^+$ may be written as $x^2 + y^2$ (the sum of two squares) if and only if, when we write $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ as a product of distinct primes, if $p_i \equiv 3 \mod 4$ then n_i is even.

Proof. Let $n = x^2 + y^2 = (x+iy)(x-iy) = N(x+iy)$. Let $z = x + iy$, so $z = \alpha_1\alpha_2...\alpha_q$ a product of irreducibles in $\mathbb{Z}[i]$.
By the proposition, each α_i is either $\alpha_i = p$ prime number with $p \equiv 3 \mod 4$, or $N(\alpha_i) = p$ a prime number which is either 2 or $\equiv 1 \mod 4$.

$$n = x^2 + y^2 = N(z) = N(\alpha_1)N(\alpha_2)...N(\alpha_q)$$

Each $N(\alpha_i)$ satisfies: either
• $N(\alpha_i) = p^2$ with $p \equiv 3 \mod 4$ prime, or
• $N(\alpha_i) = p$ with $p = 2$ or $p \equiv 1 \mod 4$ prime.
So if p^m is the largest power of p dividing n, we find that m must be even if $p \equiv 3 \mod 4$.

Conversely, let $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ be a product of distinct primes.
For each p_i, either $p_i \equiv 3 \mod 4$ and n_i is even, so $p_i^{n_i} = \left(p_i^2\right)^{\frac{n}{2}} = N\left(p_i^{\frac{n}{2}}\right)$, or $p_i = 2$ or $p_i \equiv 1 \mod 4$, then $p_i = N(\alpha_i)$ for some $\alpha_i \in \mathbb{Z}[i]$. So $p_i^{n_i} = N(\alpha_i^{n_i})$.
So n is the norm of some $z \in \mathbb{Z}[i]$, so $n = N(z) = N(x+iy) = x^2 + y^2$ is a sum of squares. □

Example. $65 = 5 \cdot 13$.
Then $5 = (2+i)(2-i)$
$13 = (2+3i)(2-3i)$.
So $65 = N((2+i)(2+3i)) = N(1+8i) = 1^2 + 8^2$.
Also $65 = N((2+i)(2-3i)) = N(7-4i) = 7^2 + 4^2$.

2.7 Algebraic integers

Definition. $\alpha \in \mathbb{C}$ is called an *algebraic integer* if it is a root of a monic polynomial in $\mathbb{Z}[x]$, i.e. $\exists$ monic $f \in \mathbb{Z}[x]$ s.t. $f(\alpha) = 0$.
Write $\mathbb{Z}[\alpha] \leq \mathbb{C}$ for the smallest subring containing α.
In other words,$\mathbb{Z}[\alpha]$=$Im(\varphi)$ where φ is defined as:

$$\begin{aligned} \varphi :& \mathbb{Z}[x] \to \mathbb{C} \\ & g \to g(\alpha) \end{aligned}$$

So also $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/I$, $I = \ker(\varphi)$.

Proposition. If $\alpha \in \mathbb{C}$ is an algebraic integer then

$$I = \ker\left(\varphi : \begin{array}{ll} \mathbb{Z}[x] & \to \mathbb{C} \\ f & \to f(\alpha) \end{array}\right)$$

is a principal ideal and is generated by a monic irreducible polynomial $f_\alpha \in \mathbb{Z}[x]$, called the *minimal polynomial* of α.

Proof. By definition there is a monic $f \in \mathbb{Z}[x]$ s.t. $f(\alpha) = 0$. So $f \in I$ so $I \neq 0$.
Let $f_\alpha \in I$ be a polynomial of minimal degree. We may suppose that f_α is primitive by dividing by its content.
We want to show that $I = (f_\alpha)$ and that f_α is irreducible.
Let $h \in I$. In $\mathbb{Q}[x]$ we have a Euclidean algorithm, so we may write $h = f_\alpha \cdot q + r$ with $r = 0$ or $\deg(r) < \deg(f_\alpha)$.
We may multiply by some $a \in \mathbb{Z}$ to clear denominators and get

$$a \cdot h = f_\alpha \cdot (aq) + (ar)$$

with aq and ar in $\mathbb{Z}[x]$.
Evaluate at α gives

$$\begin{aligned} ah(\alpha) &= f_\alpha(\alpha)(aq)(\alpha) + (ar)(\alpha) \\ &\implies 0 = (ar)(\alpha) \end{aligned}$$

So $(ar) \in I$.
As $f_\alpha \in I$ has minimal degree, we cannot have $\deg(r) = \deg(ar) < \deg(f_\alpha)$. So instead must have $r = 0$.
So $ah = f_\alpha \cdot (aq) \in \mathbb{Z}[x]$.
Take contents of everything, get

$$a \cdot c(h) = c(ah) = c(f_\alpha(aq)) = c(aq)$$

as f_α is primitive.
So $a | c(aq)$, so $aq = a\bar{q}$ with $\bar{q} \in \mathbb{Z}[x]$ and cancelling a shows $q = \bar{q} \in \mathbb{Z}[x]$.
So $h = f_\alpha \cdot q \in (f_\alpha) \lhd \mathbb{Z}[x]$. So $I = (f_\alpha)$.

Now we want to show that f_α is irreducible. We have

$$\mathbb{Z}[x]/(f_\alpha) = \mathbb{Z}[x]/\ker(\varphi) \cong Im(\varphi) = \mathbb{Z}[\alpha] \leq \mathbb{C}$$

$\mathbb{C}$ is an integral domain, so $\text{Im}(\varphi)$ is an integral domain, so $\mathbb{Z}[x]/(f_\alpha)$ is an integral domain.
So (f_α) is prime. So f_α is prime, so irreducible. □

Example. $\alpha = i$ is an algebraic integer with $f_\alpha = x^2 + 1$.
$\alpha = \sqrt{2}$ is an algebraic integer with $f_\alpha = x^2 - 2$.
$\alpha = \frac{1}{2}\left(1 + \sqrt{-3}\right)$ is an algebraic integer with $f_\alpha = x^2 - x + 1$.
The polynomial $x^5 - x + d \in \mathbb{Z}[x]$ with $d \in \mathbb{Z}$ has precisely one real root α, which is an algebraic integer.

Remark. (Galois theory)
This α cannot be constructed from $\mathbb{Z}$ using $+, -, \times, /, \sqrt[n]{}$.

Lemma. If $\alpha \in \mathbb{Q}$ is an algebraic integer, then $\alpha \in \mathbb{Z}$.

Proof. Let $f_\alpha \in \mathbb{Z}[x]$ be the minimal polynomial, which is irreducible.
In $\mathbb{Q}[x]$, $x - \alpha$ must divide f_α, but by Gauss' lemma, $f_\alpha \in \mathbb{Q}[x]$ must be irreducible.
So must have $f_\alpha = x - \alpha \in \mathbb{Z}[x]$ (else there is a proper decomposition). So $\alpha \in \mathbb{Z}$. □

2.8 Hilbert basis theorem

A ring R satisfies the *ascending chain condition (ACC)* if whenever

$$I_1 \subset I_2 \subset \ldots$$

is an increasing sequence of ideals, then we have

$$I_n = I_{n+1} = I_{n+2} = \ldots$$

for some $n \in \mathbb{N}$.
A ring satisfying this condition is called Noetherian.

Example. Any finite ring, any field, and $\mathbb{Z}$ or any other PID is Noetherian (see next proposition).
Consider $\mathbb{Z}[x_1, x_2, \ldots]$. Note that

$$(x_1) \subset (x_1 x_2) \subset (x_1 x_2 x_3) \subset \ldots$$

while none of the ideals are equal. Thus $\mathbb{Z}[x_1, x_2, \ldots]$ is not Noetherian.

Proposition. A ring R is Noetherian $\iff$ every ideal of R is finitely generated, i.e. $I = (r_1, \ldots, r_n)$ for some $r_1, \ldots, r_n \in R$ for every ideal $I \subset R$.

Proof. Suppose every ideal of R is finitely generated. Given $I_1 \subset I_2 \subset \ldots$, consider the ideal

$$I = I_1 \cup I_2 \cup \ldots$$

We have $I = (r_1, \ldots, r_n)$, with WLOG $r_i \in I_{k_i}$.
Now let $k = max\,(k_1, \ldots, k_n)$.
Then $r_1, \ldots, r_n \in I_k$, hence $I_k = I$.

On the other hand, suppose an ideal I is not finitely generated.
Choose $r_1 \in I$. Then $(r_1) \neq I$ as I is not finitely generated. Then choose $r_2 \in I \setminus (r_1)$. Then $(r_1, r_2) \neq I$. Then choose $r_3, r_4, ...$ similarly. But now we get a chain of ideals

$$(r_1) \subset (r_1, r_2) \subset ...$$

while none of them is equal to any other. Contradiction. So I must be finitely generated.

Alternative proof for second part (2017 Lent): conversely, suppose R is Noetherian. Let I be an ideal.

Choose $a_1 \in I$. If $I = (a_1)$ then done, so suppose not. Then choose $a_2 \in I \setminus \{a_1\}$; if $I = (a_1, a_2)$ then done, so suppose not... If we can't be finished by this process, then we get

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq ...$$

which is impossible as R is Noetherian. So $I = (a_1, a_2, ..., a_r)$ for some r. □

Theorem. (Hilbert's basis theorem)
R is Noetherian $\implies$ $R[x]$ is Noetherian.
(hence e.g. $Z[x]$ is Noetherian, whence $Z[x, y]$ is Noetherian, etc.)

Proof. (Lent 2017)
Let $J \lhd R[x]$. Let $f_1 \in J$ be a polynomial of minimal degree. If $J = (f_1)$ then done, else choose $f_2 \in J \setminus (f_1)$ of minimal degree. If $J = (f_1, f_2)$ then done... Suppose this never terminates, i.e. we have $(f_1) \subsetneq (f_1, f_2) \subsetneq ... \subsetneq (f_1, f_2, f_3) \subsetneq ....$

Let $0 \neq a_i \in R$ be the coefficient of the largest power of X in f_i, and consider the chain of ideals $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset ... \lhd R$. As R is Noetherian, this chain stabilizes, i.e. there exist m s.t. all a_i lie in $a_1, ..., a_m$. In particular, $a_{m+1} = \sum_{i=1}^n a_i b_i$ for some $b_i \in R$.

Let $g = \sum_{i=1}^m b_i f_i X^{\deg(f_{m+1}) - \deg(f_i)}$ has top term $\sum_{i=1}^n b_i a_i X^{\deg(f_{m+1})}$, i.e. $a_{m+1} X^{\deg(f_{m+1})}$.

Note that $f_{m+1} - g$ has degree strictly smaller than that of f_{m+1}. But $g \in (f_1, ..., f_m)$, while $f_{m+1} \notin (f_1, ..., f_m)$. So $f_{m-1} - g \notin (f_1, ..., f_m)$, contradicting with the fact that we have chosen f_{m+1} to be the minimal degree each time. □

Proof. (Lent 2016)
Let I be an ideal in $R[x]$. For $n = 0, 1, 2, ...$, let

$$I_n = \{r \in R : \exists f \in I \text{ with } f = rx^n + ...\} \cup \{0\}$$

Then each I_n is an ideal of R.
Also $I_n \subset I_{n+1} \forall n$ since $f \in I \implies xf \in I$ (as I is an ideal in $R[x]$).
Thus $I_N = I_{N+1} = ...$ for some N since R is Noetherian.
For each $0 \leq n \leq N$, we have

$$I_n = \left(r_1^{(n)}, r_2^{(n)}, ..., r_{k(n)}^{(n)} \right)$$

As R is Noetherian.
For each $r_i^{(n)}$, choose a $f_i^{(n)}$ with $f_i^{(n)} = r_i^{(n)} x^n + ...$
• Claim: The polynomials $f_i^{(n)}$ $(0 \le n \le N, 1 \le i \le k(n))$ generate I.
Proof of claim: Suppose not. Then choose $g \in i$ of minimum degree that is not generated by the above polynomials $f_i^{(n)}$.
• If $\deg(g) = n \le N$: have $g = rx^n + ...$ But $r \in I_n$. So $r = \sum_i \lambda_i r_i^{(n)}$ for some $\lambda_i \in R$.
So $\sum_i \lambda_i f_i^{(n)} = rx^n + ...$, whence $g - \sum_i \lambda_i f_i^{(n)}$ has smaller degree than g(or it's zero) and is also not in I, contradicting with the fact that g has the minimum degree.
• If $\deg(g) = n > N$: Have $g = rx^n + ...$ But $r \in I_n = I_N$, so $r = \sum_i \lambda_i r_i^{(N)}$ for some $\lambda_i \in R$.
So $x^{n-N} \sum_i \lambda_i r_i^{(N)} = rx^n + ...$ is in the ideal, whence $g - x^{n-N} \sum_i \lambda_i r_i^{(N)}$ has smaller degree than g (or it's zero) and is also not in I. Contradiction. □

Does R Noetherian imply every subring of R is Noetherian?
The answer is NO – e.g. take $\mathbb{Z}[x_1, x_2, ...]$ (an integral domain) and let R be its field of fractions, while the latter is a field so Noetherian, but the first one isn't Noetherian.

Proposition. Let R be Noetherian, I be an ideal in R. Then R/I is Noetherian.

Proof. Let

$$\begin{aligned} \varphi :& R \to R/I \\ & x \to x + I \end{aligned}$$

Given an ideal J in R/I, have $\varphi^{-1}(I)$ an ideal in R (by ideal correspondence).
So $\varphi^{-1} = (r_1, ..., r_n)$ for some $r_1, ..., r_n \in R$ (since R is Noetherian so I is finitely generated).
Thus $J = (\varphi(r_1), \varphi(r_2), ..., \varphi(r_n))$ is finitely generated. So R/I is Noetherian. □

What about $Z[x]$? (recall that it's not a pid since $(2, x)$ is not principal)

Remark. Let $E \subset F[x_1, x_2, ..., x_n]$ be any set of polynomial equations.
Consider $(E) \triangleleft F[x_1, x_2, ..., x_n]$. By Hilbert's basis theorem, there is a finite list $f_1, ..., f_k$ s.t. $(E) = (f_1, ..., f_k)$.
Given $(\alpha_1, \alpha_2, ...\alpha_n) \in F^n$, consider

$$\varphi_\alpha : \begin{pmatrix} F[x_1, ..., x_n] & \to F \\ x_i & \to \alpha_i \end{pmatrix}$$

a ring homomorphism.
$(\alpha_1, ...\alpha_n) \in F^n$ is a solution to the equations $E \iff (E) \subset \ker(\varphi_\alpha) \iff (f_1, ..., f_n) \triangleleft \ker(\varphi_\alpha) \iff (\alpha_1, ..., \alpha_n)$ is a common solution to $f_1, ..., f_k$.

3 Modules

3.1 Definitions and examples

Definition. Let R be a commutative ring. A quadruple $(M, +, 0_M, \cdot)$ is a $R-$module if:
• (M1) $(M, +, 0_M)$ is an abelian group;
• (M2) The operation $- \cdot - : R \times M \to M$ satisfies

$$\begin{aligned}
&(r_1 + r_2) \cdot m = (r_1 \cdot m) + (r_2 \cdot m) \\
&r \cdot (m_1 + m_2) = (r \cdot m_1) + (r \cdot m_2) \\
&r_1 \cdot (r_2 \cdot m) = (r_1 \cdot r_2) \cdot m \\
&1_R \cdot m = m
\end{aligned}$$

Example. 1) Let F be a field. An $F-$module is precisely the same as a vector space over F.
2) For any ring R, $R^n = R \times R \times ... \times R$ is a $R-$module via

$$r \cdot (r_1, r_2, ..., r_n) = (r \cdot r_1, r \cdot r_2, ..., r \cdot r_n)$$

3) If $I \triangleleft R$ is an ideal, then it is an $R-$module via

$$r \cdot_M a = r \cdot_R a$$

Also, R/I is a $R-$module via

$$r \cdot (a + I) = r \cdot a + I$$

4) A $\mathbb{Z}-$module is precisely the same as an abelian group. For A an abelian group,

$$\left(\begin{array}{ll} \mathbb{Z} \times A & \to A \\ (n, a) & \to \left\{ \begin{array}{ll} a + a + ... + a \text{ (n times)} & a > 0 \\ 0 & a = 0 \\ (-a) + (-a) + ... + (-a) \text{ (n times)} & a < 0 \end{array} \right. \end{array} \right)$$

5) Let F be a field, V a vector space on F, and $\alpha : V \to V$ be a linear map. Then V is a $F[x]-$module via

$$\left(\begin{array}{ll} F[x] \times V & \to V \\ (f, v) & \to (f(\alpha))(v) \end{array} \right)$$

i.e. Substitute α in the polynomial f, then act on v.
Different choices of α make V into different $F[x]-$modules, so this is a module structure.
6) If $\varphi : R \to S$ is a ring homomorphism, then any $S-$module M may be considered as a $R-$module via

$$\left(\begin{array}{ll} R \times M & \to M \\ (r, m) & \to \varphi(r) \cdot m \end{array} \right)$$

Definition. If M is a $R-$Module, a subset $N \subset M$ is a $R-$submodule if it is a subgroup of $(M, +, 0_M)$ and if $n \in N$ and $r \in R$ then $r \cdot n \in N$.
We write $n \leq M$.

Example. A subset of the R is a submodule of the $R-$module R *precisely* if it is an ideal.
A subset of an $F-$module V for F a field is a submodule *precisely* if it is a vector subspace.

Definition. If $N \subseteq M$ is a $R-$submodule, the *quotient module* M/N is the set of $N-$cosets in the abelian group $(M, +, 0_M)$ with

$$r \cdot (m + N) = r \cdot m + N$$

This is well defined as, if any two different m represent the same coset then they differ by some $n \in N$.

Definition. A function $f : M \to N$ between $R-$modules is an $R-$*module homomorphism* if it is a homomorphism of abelian groups, and satisfies

$$f (r \cdot m) = r \cdot f (m)$$

Example. If F is a field and V, W are $F-$modules (vector spaces over F), then an $F-$module homomorphism is precisely an $F-$linear map.

Theorem. (First isomorphism theorem)
Let $f : M \to N$ be a $R-$module homomorphism. Then

$$\ker (f) = \{m \in M | f (m) = 0\} \leq M$$

(submodule),

$$Im (f) = \{n \in N | \exists m \in M s.t. n = f (m)\} \leq N$$

Moreover, $M/\ker (f) \cong \mathrm{Im}(f)$.

Theorem. (Second isomorphism theorem)
Let $A, B \leq M$. Then

$$A + B = \{m \in M | \exists a \in A, b \in B \text{ s.t. } m = a + b\} \leq M$$

(a submodule), and

$$A \cap B \leq M$$

and

$$A + B/A \cong B/(A \cap B).$$

Theorem. (Third isomorphism theorem)
If $N \leq L \leq M$, then

$$M/L \cong (M/N)/(L/N).$$

In addition, there is a submodule correspondence between submodules of M/N and submodules of M which contain N.

Definition. Let M be a $R-$module, $m \in M$. The *annihilator* of m is

$$\text{Ann}\,(m) = \{r \in R | r \cdot m = 0\}$$

The annihilator of M is

$$\text{Ann}\,(M) = \bigcap_{m \in M} \text{Ann}\,(m) = \{r \in R | r \cdot m = 0 \forall m \in M\}$$

Remark. $\text{Ann}\,(m)$ is an ideal of R (so $\text{Ann}\,(M)$ is too).

Definition. If M is a $R-$module and $m \in M$, the *submodule granted by* m is

$$R_m = \{r \cdot m \in M | r \in R\}$$

Consider the $R-$module homomorphism

$$\varphi : \begin{pmatrix} R & \to M \\ r & \to r \cdot m \end{pmatrix}$$

Here

$$R_m = Im\,(\varphi)$$
$$\text{Ann}\,(m) = \ker\,(\varphi)$$

So

$$R_m \cong R / \text{Ann}\,(m)$$

Definition. Say an $R-$module M is *finitely generated* if there are elements $m_1, ..., m_k$ s.t.

$$\begin{aligned} M &= R_{m_1} + R_{m_2} + ... + R_{m_k} \\ &= \{r_1 m_1 + r_2 m_2 + ... + r_k m_k | r_1, r_2, ..., r_k \in R\} \end{aligned}$$

Lemma. A $R-$module M is finitely generated if and only if there is a surjective $R-$module homomorphism

$$f : R^k \to M$$

Proof. If $M = R_{m_1} + ... + R_{m_k}$, define

$$f : \begin{pmatrix} R^k & \to M \\ (r_1, ..., r_k) & \to r_1 m_1 + r_2 m_2 + ... + r_k m_k \end{pmatrix}$$

This is a $R-$module map. This *is* surjective by the definition of M.
Conversely, given a surjection $f : R^k \to M$, let

$$M_i = f\,(0, 0, ..., 0, 1, 0, ..., 0)$$

where the 1 is in the i^{th} position.
Let $m \in M$. As f is surjective, $m = f\,(r_1, r_2, ..., r_k)$ for some $r_1, ..., r_k$.
Then write

$$\begin{aligned} f\,(r_1, ..., r_k) &= f\,((r_1, 0, ..., 0) + (0, r_2, 0, ..., 0) + ... + (0, 0, ..., 0, r_k)) \\ &= f\,(r_1 \cdot 1, 0, ..., 0) + f\,(0, r_2 \cdot 1, 0, ..., 0) + ... + f\,(0, ..., 0, r_k \cdot 1) \\ &= r_1 f\,(1, 0, ..., 0) + r_2 f\,(0, 1, 0, ..., 0) + ... + r_k\,(0, ..., 0, 1) \\ &= r_1 m_1 + r_2 m_2 + ... + r_k m_k \end{aligned}$$

So the m_i's generate M. ☐

Corollary. If $N \leq M$ and M is finitely generated, then M/N is finitely generated.

Proof. m is finitely generated
$\implies$ there is a surjection $f : R^k \to M$
$\implies$ $R^k \to M \to M/N$ (by $m \to m + N$) (surjection) □

Example. A submodule of a finitely generated module need not be finitely generated.
Let

$$R = \mathbb{C}[x_1, x_2, x_3, ...]$$

Let $M = R$ be finitely generated (by 1). The submodule $I = (x_1, x_2, ...) \lhd R$ is not finitely generated (because finitely generated as a module implies finitely generated as an ideal, which it isn't).

Example. For $\alpha \in \mathbb{C}$, $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module $\iff$ α is an algebraic integer (see example sheet).

3.2 Direct sums and free modules

Definition. If $M_1, M_2, ..., M_k$ are $R-$modules, the *direct sum*

$$M_1 \oplus M_2 \oplus ... \oplus M_k$$

is the set

$$M_1 \times M_2 \times ... \times M_k$$

with addition

$$(m_1, m_2 ..., m_k) + (m_1', m_2', ..., m_k') = (m_1 + m_1', ..., m_k + m_k')$$

and R-module structure

$$r \cdot (m_1, ..., m_k) = (r \cdot m_1, r \cdot m_2, ..., r \cdot m_k)$$

Example. What we have been calling R^n is $R \oplus R \oplus ... \oplus R$ (n times).

Definition. Let $m_1, m_2, ..., m_k \in M$. The set $\{m_1, ..., m_k\}$ is *independent* if

$$\sum_{i=k}^{m} r_i m_i = 0 \implies r_1 = r_2 = ... = r_k = 0$$

Definition. A subset $S \subset M$ *generates M freely* if
1) S generates M;
2) Any function $\psi : S \to N$ to a $R-$module extends to a $R-$module map $\theta : M \to N$.
If θ_1 and θ_2 are two of such extensions, consider $\theta_1 - \theta_2 : M \to N$. Then $S \subseteq \ker(\theta_1 - \theta_2) \leq M$. So the submodule generated by S lies in $\ker(\theta_1 - \theta_2)$ too. But 1) says S generates M. So $M = \ker(\theta_1 - \theta_2)$. So $\theta_1 = \theta_2$.
A $R-$module freely generated by some subset $S \subset M$ is called *free*, and S is called a *basis*.

Proposition. For a subset $\{m_1, m_2, ..., m_k\} \subset M$, the following are equivalent:
1) S generates M freely;
2) S generates M and the set S is independent;
3) Every element of M is *uniquely* expressible as

$$r_1m_1 + r_2m_2 + ... + r_km_k$$

for some $r_i \in R$.

Proof. • 1) $\implies$ 2):
Let S generate M freely.
If S is *not* independent, we have

$$0 = r_1m_1 + ... + r_km_k$$

with some $r_j \neq 0$.
Let

$$\psi : \begin{pmatrix} S \to & R \\ m_j \to & 1_R \\ m_i \to & 0\ (i \neq j) \end{pmatrix}$$

a function.
As S generates M freely, this extends to a $R-$module homomorphism $\theta : M \to R$.
Thus

$$\begin{aligned} 0 = \theta(0) &= \theta(r_1m_1 + r_2m_2 + ... + r_km_k) \\ &= r_1\theta(m_1) + ... + r_k\theta(m_k) \\ &= r_j \cdot 1_R \in R \end{aligned}$$

a contradiction as we supposed $r_j \neq 0$.

The remaining steps are just as in Linear Algebra. □

Example. The set $\{2, 3\} \in \mathbb{Z}$ generates $\mathbb{Z}$, but *not* freely, as $3 \cdot 2 + (-2) \cdot 3 = 0$. So S is not independent. So S doesn't generate $\mathbb{Z}$ freely. Also $\{2\}$ and $\{3\}$ do *not* generate $\mathbb{Z}$.

Example. The $\mathbb{Z}$-module $\mathbb{Z}/2$ is not free.
Generating set: $\{1\}$, $\{0, 1\}$.
1) for $\{1\}$: Let

$$\psi : \begin{pmatrix} \{1\} & \to \mathbb{Z} \\ 1 & \to 1 \end{pmatrix}$$

this extends to

$$\theta : \begin{pmatrix} \mathbb{Z}/2 & \to \mathbb{Z} \\ 1 & \to 1 \\ 0 = 1 + 1 & \to 1 + 1 \end{pmatrix}$$

which is a contradiction since it's not a homomorphism.
For the second case is generally the same.

Lemma. If $S = \{m_1, ..., m_k\} \subset M$ is freely generated, then $M \cong R^k$ as an $R-$module.

Proof. Let $f : R^k \to M$ by $(r_1, ..., r_k) \to \sum r_i m_i$ as $R-$module map. It is surjective as $\{m_i\}$ generate M, and is injective as the m_i are independent. □

Definition. If M is a finitely generated $R-$module, we have shown that there is a surjective $R-$module homomorphism $\varphi : R^k \to M$.
We call $\ker(\varphi)$ the *relation module* for these generators.
Now As $M \cong R^k / \ker(f)$, knowing M is equivalent ot knowing the relation module.
We say M is *finitely presented* if, in addition, $\ker(\varphi)$ is finitely generated.
More precisely, if $\{m_1, m_2, ..., m_k\}$ generate M and $\{n_1, n_2, ..., n_l\}$ generate $\ker(\varphi)$, then each $n_i = (r_{i1}, r_{i2}, ..., r_{ik})$ corresponds to the relation

$$r_{i1}m_1 + r_{i2}m_2 + ... + r_{ik}m_k = 0$$

in M.

Proposition. (Invariance of dimension (rank))
Let R be a non-zero ring. Then if $R^n \cong R^m$ as a $R-$module, we must have $n = m$.

Proof. We know this is true if R is a field (since they are vector spaces).
General construction: let $I \lhd R$ be an ideal and M a $R-$module. Define

$$IM = \{a \cdot m \in M | a \in I, m \in M\}$$

a submodule of M, so M/IM is a $R-$module.
If $b \in I$ then $b \cdot (m + IM) = b \cdot m + IM = 0 + IM$.
So M/IM is a R/I-module via

$$(r + I) \cdot (m + IM) = r \cdot m + IM$$

General property: every non-zero ring has a maximal ideal.
Observation: an ideal $I \lhd R$ is proper $\iff 1_R \notin I$.
So an increasing union of proper ideals is proper.
(Fact: (Zorn's lemma applies) so there is a maximal ideal)
Back to the proof: choose a maximal ideal $I \lhd R$.
If $R^n \cong R^m$, then $R^n/IR^n \cong R^m/IR^m$, i.e. $(R/I)^n \cong (R/I)^m$. But I is maximal, so R/I is a field. So this is an isomorphism between vector spaces over the spaces R/I. So $n = m$ by usual dimension theory from linear algebra. □

3.3 Matrices over Euclidean domains

Until further notice, R is a Euclidean domain, and write $\phi : R \backslash \{0\} \to \mathbb{Z} \geq 0$ for its Euclidean function.
We know what $\gcd(a, b)$ is for $a, b \in R$ and is unique up to associates. The Euclidean algorithm using ϕ shows that $\gcd(a, b) = ax + by$ for some $x, y \in R$.

Definition. *Elementary row operations* on a $m \times n$ matrix A with entries in R are

(ER1) Add $c \in R$ times the i^{th} row to the j^{th}. This may be done by multiplying A on the left by

$$\begin{pmatrix} 1 & & & & \\ & 1 & & c & \\ & & 1 & & \\ & & & ... & \\ & & & & 1 \end{pmatrix}$$

Where c is in the j^{th} row and the i^{th} column.
(ER2) Swap the i^{th} and the j^{th} rows. This is done using

$$\begin{pmatrix} 1 & & & & & \\ & 0 & & 1 & & \\ & & 1 & & & \\ & 1 & & 0 & & \\ & & & & ... & \\ & & & & & 1 \end{pmatrix}$$

Where the two 1 are in the (i, j) entry and the (j, i) entry.
(ER3) Multiply the i^{th} row by a *unit* $c \in R$, using

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & c & & \\ & & & ... & \\ & & & & 1 \end{pmatrix}$$

Where c is in the (i, i) entry.

We have analogues for column operations, called (EC1),(EC2),(EC3).

Definition. A and B are *equivalent* if they differ by a sequence of elementary row or column operations.
If A and B are equivalent, there are invertible (square) matrices P,Q s.t. $B = QAP^{-1}$.

Theorem. (Smith normal form)
A $m \times n$ matrix A on a ED R is equivalent to $\text{Diag}(d_1, d_2, ..., d_r, 0, ..., 0)$ with the d_i all non-zero and

$$d_1|d_2|...|d_r$$

The d_k are called *invariant factors* of A.

Proof. if $A = 0$ we are done. So suppose $A \neq 0$.
So some entry $A_{ij} \neq 0$. Swapping the i^{th} and first row then j^{th} and first column, we arrange that $A_{11} \neq 0$.
Try to reduce $\varphi(A_{11})$ as much as possible:
Case 1) If there is a A_{1j} not divisible by A_{11}, use Euclidean algorithm to write

$$A_{1j} = q \cdot A_{11} + r$$

with $\varphi(r) < \varphi(A_{11})$.
Subtract q times the first column from the j^{th} column. In position $(1, j)$, we

now have r. Swapping j^{th} and 1^{st} columns puts r in position $(1,1)$, and so $\varphi(r) < \varphi(A_{11})$.
Case 2) If there is a A_{i1} not divisible by A_{11}, do the analogous thing to reduce $\varphi(A_{11})$.
After finitely many applications of Case 1 and Case 2, we get that A_{11} divides all A_{ij} and all A_{i1}.
Then subtracting appropriate multiples of the first column from all others makes $A_{1j} = 0$ for all j apart from the first one. Do the same with rows. Then we have

$$\begin{pmatrix} d & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & & & \\ \dots & & & C & \\ 0 & & & & \end{pmatrix}$$

Case 3) if there is an entry of C not divisible by d, say A_{ij} with $i > 1, j > 1$. Then write $A_{ij} = qd + r$, with $\varphi(r) < \varphi(d)$.
Now add column 1 to column j, subtract q times row 1 from row i, swap row i with row 1, and swap column j with column 1.Then the $(1,1)$ entry is r, and $\varphi(r) < \varphi(d)$.
But now the zeroes are messed up. So do case 1 and case 2 if necessary to get

$$\begin{pmatrix} d' & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & & & \\ \dots & & & C' & \\ 0 & & & & \end{pmatrix}$$

But now with $\varphi(d') \leq \varphi(r) < \varphi(d)$.
Since case 3 strictly decreases $\varphi(d)$, it can only happen for finitely many times.
Therefore, we arrive at

$$\begin{pmatrix} d & 0 & 0 & \dots & 0 \\ 0 & & & & \\ 0 & & & & \\ \dots & & & C & \\ 0 & & & & \end{pmatrix}$$

Such that d divides *every* entry of C (this is because case 3 stops only if there is no entry of C not divisible by d, by the condition).
Now apply the entire process to C. We end up with a diagonal matrix with the claimed divisibility. □

Example.

$$\begin{pmatrix} 3 & 7 & 4 \\ 1 & -1 & 2 \\ 3 & 5 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 2 \\ 3 & 7 & 4 \\ 3 & 5 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 3 & 10 & -2 \\ 3 & 8 & -5 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & -2 \\ 0 & 8 & -5 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 10 \\ 0 & 5 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 10 \\ 0 & 1 & -12 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -12 \\ 0 & 2 & 10 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 34 \end{pmatrix}$$

To study the uniqueness of the invariant factors (the d_k's) of a matrix A, we will consider *minors*:

Definition. A $k \times k$ *minor* of a matrix A is the determinant of a $k \times k$ sub-matrix of A (a matrix found by removing all but k rows and all but k columns).
For a matrix A, the k^{th} *fitting ideal* called $\mathrm{Fit}_k(A) \lhd R$ is the ideal generated by the set of all $k \times k$ minors of A.

Lemma. If A and B are equivalent matrices, then

$$\mathrm{Fit}_k(A) = \mathrm{Fit}_k(B)$$

for all k.

Proof. We just show that changing A by the elementary row operations (or the column versions) doesn't change $\mathrm{Fit}_k(A)$. We just need to consider the row operations as $\mathrm{Fit}_k(A) = \mathrm{Fit}_k\left(A^T\right)$.
For (ER1): Fix C a $k \times k$ minor of A. Let B be the result of adding c times the i^{th} row to the j^{th} row.
If the j^{th} row is outside of C, then the minor is unchanged.
If i^{th} and j^{th} row are *in* C, then the sub-matrix changes by a row operation. But we know from linear algebra that a row operation doesn't change the determinant.
If j^{th} row is in C but the i^{th} row is not, then C is changed to C' with j^{th} row equal to

$$(C_{j1} + cf_1, C_{j2} + cf_2, ..., c_{jk} + cf_k)$$

Where f_1, f_2, ... f_k are the i^{th} row.
Computing $\det(C')$ using this row, we get $\det(C') = \det(C)$ a minor $+c\det($ matrix obtained by replacing the jth row of C with $f_1, f_2, ..., f_k)$ also a minor of A.

So $\det(C') \in \mathrm{Fit}_k(A)$.
(ER2) and (ER3) follow by standard properties of swapping rows or multiplying rows on determinants.
So $\mathrm{Fit}_k(B) \leq \mathrm{Fit}_k(A)$. But this also follows in the opposite direction as row operations are invertible. So they are equal. □

Remark. if $B = \mathrm{Diag}(d_1, d_2, ..., d_r, 0, ..., 0)$ is a matrix in its Smith Normal Form, then

$$\mathrm{Fit}_k(B) = (d_1 d_2 ... d_n)$$

Corollary. If A has Smith Normal Form $\mathrm{Diag}(d_1, d_2, ..., d_r, 0, ..., 0)$ then $(d_1 d_2 ... d_k) = \mathrm{Fit}_k(A)$, so d_k is unique up to associates.

Example. Consider

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = A$$

Then

$$\mathrm{Fit}_1(A) = (2, 3) = (1)$$

So $d_1 = \pm 1$,

$$\mathrm{Fit}_2(A) = (6)$$

So

$$d_1 d_2 = \pm 6 \implies d_2 = \pm 6$$

So

$$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}$$

is a Smith Normal Form for A.

Lemma. Let R be a Euclidean Domain. Any submodule of R^m is generated by at most m elements.

Proof. Let $N \leq R^m$ be a submodule. Consider the ideal

$$I = \{r \in R | \, (r, r_2, ..., r_m) \in N \text{ for some } r_2, ..., r_m \in \mathbb{R}\}$$

As R is a ED, it is also a PID. So $I = (a)$ for some $a \in R$.
Choose a $n = (a_1, a_2, ..., a_m) \in N$.
For a $(r_1, r_2, ..., r_m) \in N$, we know $a | r_1$, so $r_1 = r \cdot a_1$, and

$$(r_1, r_2, ..., r_m) - r\,(a_1, a_2, ..., a_m) = (0, r_2 - ra_2, ..., r_m - ra_m)$$

This lies in $N' = N \cap \left(\{0\} \times R^{m-1}\right) \leq R^{m-1}$.
Then by induction we can suppose that there are $n_2, ...n_m \in N'$ generating N'.
Thus

$$(r_1, ..., r_m)$$

lies in the submodule generated by $n, n_2, ..., n_m$. Since $r_1, ..., r_m$ are arbitrary, we know that $n, n_2, ..., n_m$ generate N. □

(missing 0.5 lecture?)

Example. Let $R = \mathbb{Z}$ (a ED), and let A be the abelian group (=$\mathbb{Z}-$module) generated by a, b, c, subject to $2a + 3b + c = 0$, $a + 2b = 0$ and $5a + 6b + 7c = 0$.

Thus $A = \mathbb{Z}^3/N$ where $N \leq \mathbb{Z}^3$ generated by $(2,3,1)^T, (1,2,0)^T, (5,6,7)^T$.

Now put $M = \begin{pmatrix} 2 & 1 & 5 \\ 3 & 2 & 6 \\ 1 & 0 & 7 \end{pmatrix}$ into Smith Normal form we get $(1,1,3)$. To show that, we just have to calculate the fitting ideals: $\text{Fit}_1(M) = (1)$, $\text{Fit}_2(M) = (1)$ and $\text{Fit}_3(M) = \det(M) = 3$.

After changing basis, N is generated by $(1,0,0), (0,1,0), (0,0,3)$. So $A \cong \mathbb{Z}/3$.

3.3.1 Structure theorem for finitely-generated abelian groups

Any f.g. abelian group is isomorphic to

$$C_{d_1} \times C_{d_2} \times ... \times C_{d_r} \times C_\infty \times C_\infty \times ... \times C_\infty$$

with $d_1 | d_2 | ... | d_r$.

Proof. Apply classification of f.g. modules to the ED $R = \mathbb{Z}$, and note $\mathbb{Z}/(d) = C_d$ and $\mathbb{Z}/(0) = C_\infty$. □

Lemma. Let R be a ED, $a, b \in R$ with $gcd(a, b) = 1$. Then $R/(ab) \cong R/(a) \oplus R/(b)$.

Proof. Consider the $R-$module homomorphism

$$\begin{aligned} \phi : & R/(a) \oplus R/(b) && \to R/(ab) \\ & (r_1 + (a), r_2 + (b)) && \to (br_1 + ar_2 + (ab)) \end{aligned}$$

As $gcd(a, b) = 1$, $(a, b) = (1)$. So $1 = xa + yb$ for some $x, y \in \mathbb{Z}$. So for $r \in R$, we get $r = rxa + ryb$. So

$$r + (ab) = rxa + ryb + (ab) = \phi(ry + (a), rx + (b))$$

So ϕ is onto.

Now we also have to deal with injectivity (since $R/(ab)$ is not necessarily finite). If $\phi(r_1 + (a), r_2 + (b)) = 0 + (ab)$, then $br_1 + ar_2 \in (ab)$. Thus $a|br_1 + ar_2$, so $a|br_1$, but $gcd(a, b) = 1$, so $a|r_1$, so $r_1 + (a) = 0 + (a)$. □

3.3.2 Primary decomposition theorem

Let R be a ED, M a f.g. $R-$module. Thus $M \cong N_1 \oplus ... \oplus N_t$ with each N_i either equal to R, or $R/(p^n)$ for some prime $p \in R$ and some $n \geq 1$.

Proof. Note that if $d = p_1^{n_1}...p_k^{n_k}$ with $p_i \in R$ *distinct* primes, then the previous lemma shows that $R/(d) \cong R/(p_1^{n_1}) \oplus ... \oplus R/(p_k^{n_k})$. Plug this into the usual classification of f.g. modules we get the result. □

3.4 Modules over $F[X]$, andnormal forms for matrices

For any field F, $F[X]$ is a ED. So the results of the last section apply.

If V is a vector space over F and $\alpha : V \to V$ an endomorphism, then we have

$$\begin{aligned} F[X] \times V && \to V \\ (f, v) && \to f(\alpha)(v) \end{aligned}$$

which makes V into a $F[X]-$module, call it V_α (see section 3.1).

Lemma: if V is finite-dimensional, then V_α is finitely-generated as a $F[X]-$module.

Example. 1) Suppose $V_\alpha \cong F[X]/(X^r)$ as a $F[X]-$module. This has $F-$basis $1, X, X^2, ..., X^{r-1}$, and the action of α on V corresponds to multiplication by X.

So in this basis, α has matrix with $A_{(i+1),i} = 1$ and all other entries 0.

2) Suppose $V_\alpha \cong F[X]/(X-\lambda)^r)$is a $F[X]-$module. Consider $\beta = \alpha - \lambda Id$, then

$$V_\beta \cong F[Y]/(Y^n)$$

as a $F[Y]-$module. So by (1), V has a basis so that β is given by the above matrix. So α is given by $\text{Diag}(\lambda) + A$ where $A_{(i+1),i} = 1$.

3) Suppose $v_\alpha \cong F[X]/(f)$ with $f = a_0 + a_1 X + ... + a_{r-1}X^{r-1} + X^r$. Then $1, X, ..., X^{r-1}$ is a $F-$basis, and in this basis, α is given by the A in example (1) with an additional column $-a_0, -a_1, ..., -a_{r-1}$ added rightmost. This matrix is called the *companion matrix* for f_1 and is written $C(f)$.

3.4.1 Rational canonical form theorem

Let $\alpha : V \to V$ be a linear map, V finite-dimensional vector space over F. Regards V as a $F[X]-$module V_α, we have

$$V_\alpha \cong F[X]/(d_1) \oplus ... \oplus F[X]/(d_r)$$

with $d_1|d_2|...|d_r$. This there is a basi sof V for which α is given by $\text{Diag}(c(d_1), c(d_2), ..., c(d_r))$. To prove this we can simply apply classification of f.g. modules over $F[X]$, an ED, and note that is(?) copies of $F[X]$ appear, as this has ∞ dimension over F.

Observations:
1) If α is represented by a matrix A in some basis, then A is conjugate to $(\text{Diag}(c(d_1), ..., c(d_r))$. 2) The minimal polynomial for α is $d_r \in F[X]$.
3) The characteristic polynomial of α is $d_1 d_2 ... d_r$.

Lemma. The primes in $\mathbb{C}[X]$ are $X - \lambda$ for $\lambda \in \mathbb{C}$, up to associates.

Proof. If $f \in \mathbb{C}[X]$ is irreducible, Fundamental theorem of algebra says that f has a root λ, or f is a constant. If it is constant it is 0 or a unit X, so $X - \lambda | f$, so $f = (X - \lambda)g$. But f is irreducible. So g is a unit, so f is an associate of $X - \lambda$. □

The conjugacy classes in $GL_2(\mathbb{Z}/3)$ are

$$\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

for non-zero λ and μ.

Recall

$$|GL_2(\mathbb{Z}/3)| = (9-1)(9-3) = 2^4 \cdot 3$$

so Sylow 2-subgroup has order $16 = 2^4$. The first matrix among the above 5 has order 4, the second and third have order 8, while for the fourth one, $\lambda = 1$ has order 3 and $\lambda = 2$ has order 6, and the diagonal matrices has order 2. So Sylow 2-subgroup cannot be cyclic (order 16).

Now let A, B be the first and the second matrix respectively. Then

$$A^{-1}BA = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$$

This have to be some power of B (since it's in the same conjugacy class as B). In fact it is equal to B^3.

So $\langle B \rangle \leq \langle A, B \rangle \leq GL_2(\mathbb{Z}/3)$, and $\langle B \rangle \triangleleft \langle A, B \rangle$.

By the second isomorphism theorem is $\frac{\langle A,B \rangle}{\langle B \rangle} = \frac{\langle A \rangle}{\langle A \rangle \cap \langle B \rangle}$. But

$$\langle A \rangle \cap \langle B \rangle = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle$$

is a group of order 2. But $\langle A \rangle$ has order 4. So

$$|\langle A, B \rangle / \langle B \rangle| = |\langle A \rangle / (\langle A \rangle \cap \langle B \rangle)| = 4/2 = 2$$

so $\langle A, B \rangle | = 2 \cdot 8 = 16$. So this is a Sylow 2-subgroup of $GL_2(\mathbb{Z}/3)$. It is

$$\left\langle A, B | A^4 = I, B^8 = I, A^{-1}BA = B^3 \right\rangle$$

a *semidihedral group of order 16*.

Example. Let $R = \mathbb{Z}[X]/(X^2 + 5)$, which we wish to show, that it is equal to $\mathbb{Z}[-5] \leq \mathbb{C}$. Then

$$(1 + X)(1 - X) = 1 - X^2 = 1 + 5 = 6 = 2 \cdot 3$$

while $1 \pm X$, $2, 3$ are all irreducible, so R is *not* a UFD. Let

$$I_1 = (3, 1 + X), I_2 = (3, 1 - X)$$

be ideals (submodules) of R. Consider

$$\begin{aligned} \phi : I_1 \oplus I_2 &\to R \\ (a, b) &\to a + b \end{aligned}$$

an $R-$module map. Then

$$\mathrm{im}(\phi) = (3, 1 + X, 1 - X)$$

But $3 - ((1 + X) + (1 - X)) = 1$. So this is the whole ring.

Also $\ker(\phi) = \{(a, b) \in I_1 \oplus I_2 | a + b = 0\} \cong I_1 \cap I_2$ by sending x back to $(x, -x)$. Hence

$$(3) \subset I_1 \cap I_2$$

Let $s \cdot 3 + t(1 - x) \in (3, 1 - X) \subset R = \mathbb{Z}[X]/(X^2 + 5)$.

Working module (3) as well, get

$$t(1 + X) = (1 - X)p \pmod{(3, X^2 + 5) = (3, X^2 - 1) = (3, (X - 1)(X + 1))}.$$

So $1 - X|t$, so $(1+X)(1-X)|t(1+X)$, so $t(1+X) = q(X^2-1) = q(X^2+5-6)$ i.e. $t(1+X) = 3(-2q)$.

Therefore $s \cdot 3 + t(1+X)$ is divisible by 3, so $I_1 \cap I_2 \subset (3)$, so equality.

By Example sheet 4 Q1(iii), if we have module $N \leq M$ and $M/N \cong \mathbb{R}^n$, then $M \cong N \oplus R^n$.

So hence, $I_1 \oplus I_2 / \ker(\phi) \cong \mathrm{im}(\phi) = R$, so $I_1 \oplus I_2 \cong R \oplus \ker(\phi) = R \oplus (3)$.

Consider

$$\begin{aligned} \psi : R &\to (3) \\ x &\to 3x \end{aligned}$$

$\ker(\psi) = \{x \in R | 3x = 0\} = 0$ as R is an integral domain. So ψ is an isomorphism. So $I_1 \oplus I_2 \cong R \oplus R$.

We claim that I_1 is not principal. If $I_1 = (a + bX)$, then $I_2 = (a - bX)$. Then

$$(3) = I_1 \cap I_2 = ((a+bX)(a-bX)) = (a^2 - bX^2) = (a^2 + 5b^2)$$

so $3 \in (a^2 + 5b^2)$, so $3 = (a^2 + 5b^2)(c + dX)$, so $a^2 + 5b^2 | 3$. Contradiction. So I_1 cannot be principal, so I_2 cannot be as well. But now:

- I_1 need 2 eleemnts to generate it, but it is not the free module R^2;
- I_1 *is* a direct summand of R^2.