Groups, Rings and Modules ①

Chapter 1: Groups
- Simple Groups
- Sylow Theorems

Chapter 2: Rings
- Ideals
- Factorisation

Chapter 3: Modules
- Like Vector Spaces, over a ring
- Structure Theorem

Books
- Hartley and Hawkes, "Rings, Modules and Linear Algebra", Chapman and Hall 1970
- Fraleigh, "A First Course in Abstract Algebra", Addison-Wesley 2003
- Rose, "A Course on Group Theory", C.U.P 1978, Dover 1994
- Cameron, "Introduction to Algebra", O.U.P 1998

Chapter 0: Review from Groups 1A

Groups, subgroups, order of an element, order of a subgroup

1. $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
2. $\mathbb{Z}_n$, the integers modulo n (under addition), cyclic
3. D_{2n}, the dihedral group, symmetries of a regular n-gon (n rotations, n reflections)
4. S_n, the symmetric group, permutations of an n-point set.

5. Matrix Groups, e.g. $GL_n(\mathbb{R})$, the group of invertible $n \times n$ real matrices.

Lagrange's Theorem

If H is a subgroup of a finite group G, then $|H| \mid |G|$. This is true because the left cosets of gH partition G. $|G:H| = |G|/|H|$

Group Actions

An *action* of a group G on a set X is a function $* : G \times X \to X$ such that (writing $gx = *(g, x)$):

1. $g(hx) = (gh)x \quad \forall g, h \in G, \ \forall x \in X$
2. $e(x) = x \quad \forall x$

So each group element is permuting the set X. For example, D_{2n} acts on the regular n-gon in the obvious way: $gx = g(x)$.

For $x \in X$, we have the orbit, $\text{orb}(x) = \{gx : g \in G\}$ and the stabiliser $\text{stab}(x) = \{g \in G : gx = x\}$

In the above example D_{2n}, $\text{orb}(x) = X$, $\text{stab}(x) = \{e, \text{reflection in } x\}$

Orbit-Stabiliser Theorem $|\text{orb}(x)||\text{stab}(x)| = |G|$

Writing $H = \text{stab}(x)$, we wish to show that
$|\text{orb}(x)| = \#$ left cosets of H
We have a bijection left cosets of $H \to \text{orb}(x)$, $gH \mapsto gx$
This is well defined because $h \in H \Rightarrow gx = (gh)x$

Groups, Rings and Modules ①

Homomorphisms

A homomorphism $\theta : G \to H$ is a map that preserves the structure of a group, i.e. $\theta(gh) = \theta(g)\theta(h) \quad \forall g, h \in G$

The image $\mathrm{Im}(\theta) = \theta(G) = \{\theta(g) \mid g \in G\} \leq H$

The kernel $K = \ker(\theta) = \{g \in G : \theta(g) = e\} \trianglelefteq G$
The kernel K is always a normal subgroup of G.
$gKg^{-1} = K \quad \forall g \in G$.

$$h \in K \Rightarrow \theta(h) = e \Rightarrow \theta(ghg^{-1}) = \theta(g)\,\theta(h)\,\theta(g^{-1})$$
$$= \theta(g)\,\theta(g)^{-1} = e \Rightarrow ghg^{-1} \in K$$

This is the reason why normal subgroups are important.

Normal Subgroups

Equivalently:

1. $gHg^{-1} = H \quad \forall g \in G$ (our definition)
2. $gH = Hg \quad \forall g \in G$ (left cosets = right cosets)
3. The operation on left cosets given by $(gH)(g'H) = gg'H$ is well defined; it doesn't depend on how we wrote gH and $g'H$.

Groups, Rings and Modules ②

For H a normal subgroup of G, we can make the left cosets of H into a group by $(gH)(g'H) = gg'H$, called the Quotient group, G/H. We can view G/H as "G, but with g, g' regarded as the same if they differ by an element of H" i.e. $g = g'h$ for some $h \in H$. For example, in $\mathbb{Z}$, $7\mathbb{Z}$ is normal (as $\mathbb{Z}$ is abelian).

Elements of $\mathbb{Z}/7\mathbb{Z}$ are things like $7\mathbb{Z}+3$. View it as "$\mathbb{Z}$, with x, y regarded as the same if $x-y \in 7\mathbb{Z}$ i.e. $x \equiv y \pmod 7$)
This is precisely $\mathbb{Z}_7$. Formally, we have an isomorphism $\mathbb{Z}_7 \to \mathbb{Z}/7\mathbb{Z}$, $x \mapsto x + 7\mathbb{Z}$.

We have $\pi : G \to G/H$, $g \mapsto gH$, the projection (or quotient) map. Clearly π is surjective, and $\ker \pi = H$. So H normal means that $\exists\, \theta$, a homomorphism, $\ker \theta = H$. Thus, normal subgroups are the same as kernels of homomorphisms from G. So we can view G/H just as the image of a homomorphism on G with kernel H.

Indeed, we have the <u>Isomorphism Theorem</u>:

Given $\theta : G \to H$, $G/\ker\theta \cong \theta(G)$
(because with $H = \ker\theta$, we have an isomorphism $G/H \to \theta(G)$, $gH \mapsto \theta(g)$)

<u>Permutations</u>

Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

e.g. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 2 & 1 & 5 & 6 & 7 \end{pmatrix}$ has $\sigma = (1\ 3\ 8\ 7\ 6\ 5)$
(24

<u>The cycle type</u> means the set of its cycle lengths. Here, σ has cycle type $6 \cdot 2$.

Since every cycle is a product of transpositions, we can write every $\sigma \in S_n$ as a product of transpositions.

e.g. $\sigma = (1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5) = (1 5)(1 4)(1 3)(1$

We say σ is <u>even</u> if $\sigma = \tau_1 \tau_2 \dots \tau_{2k}$ (the τ_i are transpositio
and <u>odd</u> if $\sigma = \tau_1' \tau_2' \dots \tau_{2k+1}'$

This <u>is</u> well defined. No $\sigma \in S_n$ is both odd and even, because composing with a transposition changes the number of cycles by ± 1.

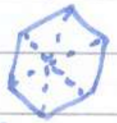
For example: $(1\ 2 \dots 9)(4\ 7) = (1\ 2\ 3\ 4\ 8\ 9)(5\ 6\ 7)$ $\uparrow 1$
and so also $(1\ 2\ 3\ 4\ 8\ 9)(5\ 6\ 7)(4\ 7) = (1\ 2 \dots 9)$ $\downarrow 1$

So $\sigma = \tau_1 \tau_2 \dots \tau_{2k} \Rightarrow$ # cycles of $\sigma \equiv n \pmod 2$
and $\sigma = \tau_1 \dots \tau_{2k+1} \Rightarrow$ # cycles of $\sigma \equiv n+1 \pmod 2$

We have the alternating group $A_n = \{\sigma \in S_n \mid \sigma \text{ even}\}$
with $|A_n| = \frac{n!}{2}$ (since $\sigma \mapsto (1 2)\sigma$ maps odd $\to$ even)

How many $\sigma \in S_6$ have cycle type 3^2? We have $6!$ ways to name such a σ. But each σ has been named $3 \times 3 \times 2$ times, so there are $6! \div (3 \times 3 \times 2)$

A subgroup of S_n is a <u>permutation group</u> (of degree n). Given a group action on a set X, we have a homomorphism $\rho : G \to S_X$ given by $\rho(g) : X \to X,\ x \mapsto gx$. Any such ρ is called a <u>permutation representation</u> of G.



e.g. Let D_{12} act on the diameters (through vertices of our hexagon) in the obvious way. So we have $\rho : D_{12} \to S_X$. If r = rotation by $180°$ then r keeps each element of X fixed i.e. $\rho(r) = e$.

Groups, Rings and Modules (2)

We say that ρ is faithful if each $g \neq e$ does something i.e. ρ is injective.

For example, the above action of D_{12} is <u>not</u> faithful, but the usual action of D_{12} (on the Hexagon) <u>is</u> faithful.

<u>Cauchy's Theorem</u> (A sort of converse to Lagrange's Theorem)

If p is prime and $p \mid |G|$, then G has an element of order p.

N.B. We do need some restriction on p, as $8 \mid |D_8|$, but D_8 has no element of order 8, and similarly, $12 \mid |S_4|$.

The proof of this theorem considers p-tuples $(x_1, \ldots, x_p)$ with $x_1 x_2 \ldots x_p = e$.

Groups, Rings and Modules (3)

Chapter 1: Groups

Conjugacy

We say that g, g' in G are *conjugate* if $g = hg'h^{-1}$ (or equivalently, $g' = h^{-1}gh$) for some $h \in G$.

e.g. in S_n, we have $\sigma(1\ 2\ 3\ 4)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4))$

So we can view hgh^{-1} as "g, but with our world view changed." (i.e. we have renamed x as $h(x)$)

e.g. In D_{2n}, write a for rotation by $\frac{2\pi}{n}$ and b for a reflection (say in L). Then, aba^{-1} is a reflection in $a(L)$. Note that here, $bab^{-1} = a^{-1}$

Also note that $(hgh^{-1})^n = h(g^n)h^{-1}$, so g and hgh^{-1} have the same order.

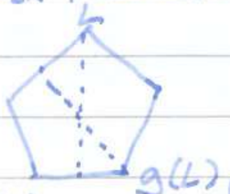
The *conjugacy class* of $g \in G$ is $ccl(g) = ccl_G(g) = \{hgh^{-1} \mid h \in G\}$

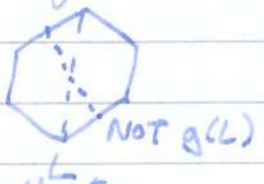
Examples

1. If G is abelian, then $ccl(g) = \{g\}$

2. In D_{2n}, $ccl(a) = \{a, a^{-1}\}$ and similarly $ccl(a^r) = \{a^r, a^{-r}\}$
So if n is even, $ccl(a^{\frac{n}{2}}) = \{a^{\frac{n}{2}}\}$ as $a^{\frac{n}{2}} = a^{-\frac{n}{2}}$

3. In D_{2n}, $ccl(b)$ = all reflections in lines $g(L)$, $g \in D_{2n}$





$$ccl(b) = \begin{cases} \text{all reflections}, & n \text{ odd} \\ \text{half of the reflections}, & n \text{ even} \end{cases}$$

Conjugation in S_n

Proposition 1 $\sigma, \tau \in S_n$ are conjugate $\Leftrightarrow$ σ, τ have the same cycle type

Proof

($\Rightarrow$) Say $\tau = \rho \sigma \rho^{-1}$. Write σ as $c_1 \dots c_k$ disjoint cycles where $c_i = (a_{i1}\, a_{i2} \dots a_{ir_i})$. Then, $\rho \sigma \rho^{-1} = c_1' \dots c_k'$, where $c_i' = (\rho(a_{i1}) \dots \rho(a_{ir_i}))$, so σ, τ have the same cycle type.

($\Leftarrow$) Given σ, τ of the same cycle type, say $\sigma = c_1 \dots c_k$ and $\tau = c_1' \dots c_k'$, where $c_i = (a_{i1} \dots a_{ir_i})$ and $c_i' = (b_{i1} \dots b_{ir_i})$, define $\rho \in S_n$ by $\rho(a_{ij}) = b_{ij}$ $\forall i, j$. Then $\rho \sigma \rho^{-1} = \tau$ $\square$

What happens in A_n?

Certainly, if $\sigma, \tau \in A_n$, conjugate in A_n, then they are conjugate in S_n so they have the same cycle type. However, the converse cannot always be true in A_n. For example, A_3 is abelian (as it is cyclic), so $(1\,2\,3)$ and $(1\,3\,2) = (1\,2\,3)^2$ are not conjugate.

Proposition 2

Let $\sigma \in A$. Then $ccl_{A_n}(\sigma) = ccl_{S_n}(\sigma)$, unless the cycle type of σ consists of only odd cycles of distinct lengths, in which case $ccl_{S_n}(\sigma)$ breaks into two conjugacy classes in A_n.

Proof

Certainly, $ccl_{A_n}(\sigma) \subset ccl_{S_n}(\sigma)$. Conversely, if σ, τ have the same cycle type, must they be conjugate in A_n?

(If so then $ccl_{A_n}(\sigma) = ccl_{S_n}(\sigma)$)

If not, then $ccl_{S_n}(\sigma)$ breaks into two conjugacy classes in A_n, namely $(\rho\sigma\rho^{-1} : \rho \text{ even})$ (any of these are trivially conjugate in A_n) and $(\rho\sigma\rho^{-1} : \rho \text{ odd})$.

Given τ of the same cycle type as σ, say $\sigma = c_1 \dots c_k$ and $\tau = c_1' \dots c_k'$, where $c_i = (a_{i1} \dots a_{ir_i})$ and $c_i' = (b_{i1} \dots b_{ir_i})$, then we define $\rho(a_{ij}) = b_{ij}$ as before.

If ρ is even, then σ, τ are conjugate in A_n. If not:

<u>If some cycle lengths are even</u>; say $c_1 = (a_1 \dots a_r)$ and $c_1' = (b_1 \dots b_r)$, then rewrite c_1' as $(b_2 b_3 \dots b_r b_1)$. Then ρ is replaced by $(b_1 b_2 \dots b_r) \circ \rho = \rho'$.

Thus, $\rho' \sigma \rho'^{-1} = \tau$, and ρ' is even, as $(b_1 \dots b_r)$ is odd. So we may assume that all the r_i are odd.

<u>If the r_i are not distinct</u>; and $r_1 = r_2$ say, then $c_1' = (b_1 \dots b_r)$, $c_2' = (d_1 \dots d_r)$. Rewrite $c_1' c_2' \dots c_k'$ as $c_2' c_1' c_3' c_4' \dots c_k'$. Then, ρ is replaced by $(b_1 d_1)(b_2 d_2) \dots (b_r d_r) \circ \rho = \rho'$.

~~Then~~

Then, $\rho' \sigma \rho'^{-1} = \tau$, and ρ' is even (as r is odd).

<u>If all the r_i are odd and distinct</u>; then the only ways to rewrite τ are to cycle symbols in each c_i separately, hence we <u>cannot</u> replace ρ by an even permutation, as a product of odd length cycles is even.

Thus, σ is <u>not</u> conjugate to $\rho\sigma\rho^{-1}$ for any odd $\rho \in S_n$ $\square$

e.g. in A_7, the cycle types are $7,\ 5\cdot 1^2,\ 4\cdot 2\cdot 1,\ 3^2\cdot 1,\ 3\cdot 2^2,\ 3\cdot 1^4,\ 2^2\cdot 1^3$

Only elements of cycle type 7 have a conjugacy class in S_7 that breaks into two in A_7.

Groups, Rings and Modules (4)

Let G be a group. G acts on itself by conjugation: $g * x = gxg^{-1}$

(This is an action: $g*(h*x) = g*(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh)*x$

The orbit of x is $ccl(x)$, so the conjugacy classes partition G, and (for G finite) have sizes dividing $|G|$ (by the Orbit-Stabiliser Theorem).

both useful

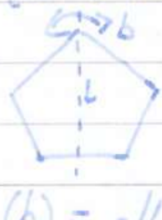
The stabiliser of x is $(g : gxg^{-1} = x) = (g : gx = xg)$ called the <u>centraliser</u> of x, written $C(x)$.

So by the Orbit-Stabiliser Theorem, $|C(x)||ccl(x)| = |G|$ (for finite G).

For G finite, say with conjugacy classes $ccl(g_1), \dots, ccl(g_r)$, we have $|ccl(g_1)| + \dots + |ccl(g_r)| = |G|$, the "class equation" of G. Using that $|ccl(g_i)| = |G|/|C(g_i)|$, this is the same as $\frac{1}{|C(g_1)|} + \dots + \frac{1}{|C(g_r)|} = 1$

e.g. in D_{2n}: $C(a) = \langle a \rangle$ = all rotations
$ccl(a) = \{a, a^{-1}\}$ (note that $n \cdot 2 = |G|$)

<u>For n odd:</u>



$C(b) = \{e, b\} = \langle b \rangle$, $ccl(b)$ = all reflections $= \{a^i b \mid 0 \le i \le n\}$

<u>For n even:</u>

reflection in the line $\perp$ to L

$C(b) = \{e, a^{\frac{n}{2}}, b, a^{\frac{n}{2}}b\}$
$ccl(b)$ = Half of all reflections $= \{a^{2i}b : 0 \le i \le \frac{n}{2}\}$

Then, the class equation for D_{2n} is :

(For n odd) $\underset{e}{1} + \underbrace{2 + \ldots + 2}_{\frac{n-1}{2} \text{ times}} + n = 2n$

(For n even) $\underset{e}{1} + \underset{a^{\frac{n}{2}}}{1} + \underbrace{2 + \ldots + 2}_{\frac{n}{2}-1 \text{ times}} + \frac{n}{2} + \frac{n}{2} = 2n$

<u>The centre</u> of G is $Z = Z(G) = \{g \in G \mid hg = gh \ \forall h\}$
$Z = \{g \in G : g \text{ commutes with all of } G\} = \{g \in G \mid ccl(g) = \{g\}\}$

e.g. 1. $Z(G) = G \Leftrightarrow G$ is abelian.

2. $Z(D_{2n}) = \begin{cases} \{e\}, & n \text{ is odd} \\ \{e, a^{\frac{n}{2}}\}, & n \text{ is even} \end{cases}$

3. $Z(S_n) = \{e\} \quad (n \geq 3)$

Note that Z is a subgroup of G, either directly or because $Z = \bigcap_{g \in G} C(g)$. Also, Z is <u>normal</u>, because if $g \in Z$, then $hgh^{-1} = g \in Z$. Alternatively, $Z = \ker \rho$, where $\rho : G \to S_n$ is the permutation representation of our action. Hence Z is normal.

A useful lemma :

<u>Lemma 3</u>

Let G be a group with centre Z. Then G/Z cyclic $\Rightarrow G$ abelian.

<u>Proof:</u>

Let gZ be a generator of G/Z, so that every left coset of Z is of the form $g^i Z$ for some $i \in \mathbb{Z}$.

Then, every element of G is of the form $g^i x$ for some $i \in \mathbb{Z}$, $x \in Z$. But $\forall i, j \in \mathbb{Z}$, $x, y \in Z$, $g^i x$ and $g^j y$ commute:

$$g^i x g^j y = g^i g^j x y = g^j g^i y x = g^j y g^i x$$

whence G is abelian. $\square$

<u>Warning</u>

It is tempting to think that G/Z abelian $\Rightarrow$ G abelian, but this is <u>false</u>.

e.g. $|Z(D_8)| = 2$, so $\frac{|D_8|}{|Z(D_8)|} = 4$, so $D_8/Z(D_8)$ is abelian, whereas D_8 is <u>not</u> abelian.

<u>Corollary</u>

Every group G of order p^2 (p prime) is abelian (a strong statement)

<u>Proof</u>

Each conjugacy class has size 1 or p or p^2. We have $|Z| = 1$, p or p^2, <u>and</u> $|Z| \equiv 0 \pmod p$ (as the sum of all conjugacy class sizes $\equiv 0 \pmod p$ and all <u>other</u> sizes are $\equiv 0 \pmod p$).

Hence, $|Z| \neq 1$, so $|Z| = p$ or p^2.

But $|Z| = p \Rightarrow |G/Z| = p \Rightarrow G/Z$ cyclic $\Rightarrow G$ abelian $\Rightarrow |Z| \neq p$ ↯

Thus $|Z| = p^2$.

Remarks

1. In fact, $G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$ (This can be done directly, see Chapter 3)

2. This does not extend to $|G| = p^3$; i.e. D_8 is not abelian.

Groups, Rings and Modules (5)

Simple Groups

A non-trivial group G is simple if it has no normal subgroups apart from $\{e\}$ and G.

For example, $\mathbb{Z}_p$ is simple (p prime). D_{2n} is not simple, and we can either see this directly, ~~or because~~ using normal subgroup $\langle a \rangle$, or notice that $\langle a \rangle$ has index 2.
(If $H \subseteq G$ has index 2, then H is normal, as left cosets = right cosets = $\{H, G/H\}$

S_n is not simple, as $A_n \trianglelefteq S_n$.

Proposition 5

G simple, abelian $\Rightarrow G \cong \mathbb{Z}_p$ for some prime p.

Proof

Choose $x \in G$, $x \neq e$. Then $\langle x \rangle$ is normal (as G is abelian), so we must have $\langle x \rangle = G$.

If $\langle x \rangle$ is infinite, then $\langle x^2 \rangle$ is a proper normal subgroup $\times$

If $\langle x \rangle$ is finite, then suppose x has order d. Then if d is prime, $G \cong \mathbb{Z}_p$.

If d is composite, choose $d' | d$ with $d' \neq 1, d$. Then $\langle x^{d'} \rangle$ is a normal subgroup $\times$ $\square$

We can now view simple groups as the building blocks for finite groups. If a finite group G is not simple, then we can

G/H
decompose G into H and ~~$G \setminus H$~~ with $H \trianglelefteq G$, then repeat if either H or G/H are not simple.

Remark

Simple groups are quite elusive, e.g. there are none of order p^2 (for p a prime). Later, we will prove that A_n is simple $\forall n$.

P-Groups

Let p be prime. G is a p group, if every element has order a power of p (e.g. any group of order p^n, by Lagrange). Do any others exist? (e.g. a 5-group of order 25).

This cannot happen as a finite group is a p-group $\Leftrightarrow |G| = p^n$ for some n (due to Cauchy)

Proposition 6

Let p be prime. Then $|G| = p^n$ (some $n \geq 1$) $\Rightarrow$ G is not simple.

Proof

By the class equation, we have $|Z(G)| \equiv 0 \pmod p$, (as every other conjugacy class not in $Z(G)$ has size $\equiv 0 \pmod p$) and so $Z(G) \neq \{e\}$

So we are done, unless $Z(G) = G$ i.e. G is abelian, and then G is not simple by proposition 5.

Corollary 7

Let p be prime, $|G| = p^n$. Then G has subgroups of all orders p^m, $0 \leq m \leq n$

<u>Note</u>: This is a converse to Lagrange.

<u>Proof</u>:

By induction on n. $n=1$ (and $n=0$) are true.

Given G with $|G| = p^n$ for some $n > 1$, we know that $Z \neq \{e\}$, so we choose $x \in Z$, $x \neq e$. WLOG, x has order p (because we can replace x by a power of x if necessary).

So $H = \langle x \rangle$ is normal (as $H \subset Z$). We have a projection map $\pi : G \to G/H$, $g \mapsto gH$

Now, $|G/H| = p^{n-1}$, so G/H has subgroups of order p^m, for $0 \leq m \leq n-1$. But for a subgroup K of G/H, we have $\pi^{-1}(K) \subset G$, with $|\pi^{-1}(K)| = p|K|$. Hence G has subgroups of all orders p^m, $1 \leq m \leq n$. $\square$

<u>Note</u>: This is a good example of when knowledge of H and G/H tells us about the whole group.

The Sylow Theorems

СИЛОВ

Let p be prime, and let $|G| = p^a m$, where $(p, m) = 1$. A subgroup of G is a <u>Sylow-p-subgroup</u> if it has order p^a (the largest power of p dividing the size of G).

e.g. in D_{50}, a Sylow-5-subgroup has order 25, e.g. the rotations

A Sylow-2-subgroup has order 2 e.g. a reflection plus e

Theorem 8 (Sylow's Theorems)

Let G be a group of order $p^a m$ where p is prime and $(p, m) = 1$

i) $\exists$ a Sylow-p-subgroup ii) All the Sylow-p-subgroups are conjugate

iii) The number n_p of Sylow-p-subgroups $\equiv 1 \pmod p$ and $n_p \mid m$.

Examples

1. $|G| = 1000 \Rightarrow G$ is not simple.

This is because $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8$, so $n_5 = 1$. Hence G has a unique subgroup of order 125. So H is normal as any conjugate $gHg^{-1} = H$ by uniqueness.

2. $|G| = 56 \Rightarrow G$ is not simple.

This is because $n_7 \equiv 1 \pmod 7$ and $n_7 \mid 8$, so $n_7 = 1$ or 8. If $n_7 = 1$, then G is not simple, as above, so WLOG let $n_7 = 8$.

The Sylow-7-subgroups meet pairwise at $\{e\}$ giving us at least $8 \times 6 = 48$ elements of order 7.

Also, by Sylow, $\exists H$, a subgroup of order 8. Now, H cannot have an element of order 7, so as $56 - 48 = 8$, it follows that H = All elements not of order 7.

Hence H is unique, and G is not simple.

Groups, Rings and Modules (6)

Corollary 9

Let p, q be primes, WLOG $p < q$. Then $|G| = pq \Rightarrow G$ not simple

Proof

$n_q \equiv 1 \pmod q$, $n_q | p \Rightarrow n_q = 1$ ($n_q \neq p$ as $p \not\equiv 1 \pmod q$, $p < q$).
The Sylow-p-subgroup is therefore unique, and hence normal. $\square$

Corollary 10

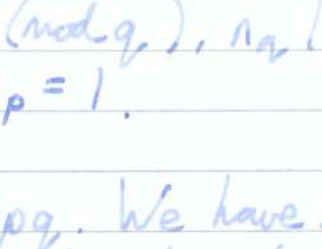
Let p, q be primes, $p < q$. $q \not\equiv 1 \pmod p \Rightarrow$ the only group of order pq is $\mathbb{Z}_{pq}$ (e.g. every group of order 15 is cyclic).

Proof

Let G be a group of order pq. Then $n_q \equiv 1 \pmod q$, $n_q | p$
$\Rightarrow n_q = 1$ (as $p \not\equiv 1 \pmod q$). Similarly, $n_p = 1$.

Every element of G has order $1, p, q$ or pq. We have exactly $p-1$ elements of order p, and exactly $q-1$ of order q (as $n_p = n_q = 1$).
But $1 + (p-1) + (q-1) < pq$ (since $p, q \geq 2$).
$\Rightarrow \exists$ an element of order pq. $\square$

For a group G, G acts on all subgroups of G by conjugation:
$g * H = gHg^{-1}$. $\text{Orb}(H) = \{gHg^{-1} : g \in G\}$ = set of all conjugates of H.
$\text{Stab}(H) = \{g \in G : gHg^{-1} = H\}$, the Normaliser of H, $N(H)$.



1. $H \subseteq N(H)$, as $hHh^{-1} = H \quad \forall h \in H$

2. $H \trianglelefteq N(H)$, normal in $N(H)$, by definition

3. $N(H)$ is the largest subgroup in which N is normal, by definition.

Example.

$S_3 \subset S_5$ (Here, $S_3 = \{\sigma \in S_5 \mid \sigma(4)=4, \sigma(5)=5\}$)
Then $(34) \notin N(S_3)$. But $(45) \in N(S_3)$ since $(45)S_3(45)^{-1} = S_3$

Proof of Theorem 8

i) We have G such that $|G| = p^a m$, $(p, m) = 1$

Let P be a maximal p-subgroup. We would like $|P| = p^a$, i.e. $|G|/|P|$ is coprime to p. We write $|G|/|P| = |G|/|N| \cdot |N|/|P|$ where $N = N(P)$. This is helpful as $|N|/|P| = |N/P|$ and $|G|/|N| = \#$ conjugates of P, by the orbit-stabiliser theorem.

We must show that $|G|/|N|$, $|N|/|P|$ are coprime to p.

For $|N|/|P|$: $\pi : N \to N/P$. If $|N/P| \equiv 0 \pmod p$ then N/P has a subgroup H of size p (Cauchy). Then $\pi^{-1}(H)$ has size $p|P|$ contradicting the maximality of P.

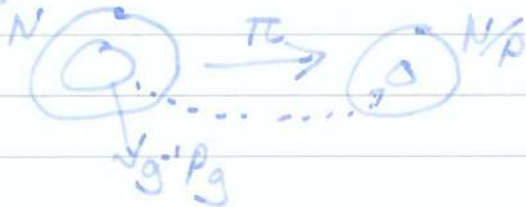
For $|G|/|N|$: Let $X = \{gPg^{-1} : g \in G\}$. We would like $|X| \not\equiv 0 \pmod p$. We have P acting on X, so that the orbits of the action have sizes $1, p, p^2, \ldots$. There is an orbit of size 1, namely $\{P\}$ since $hPh^{-1} = P \ \forall h \in P$.

Claim: There are no other orbits of size 1 (completing the proof as then $|X| \equiv 1 \pmod p$).

Proof of Claim:

Suppose $\{gPg^{-1}\}$ is an orbit of size 1. Then P fixes gPg^{-1}, i.e. $h(gPg^{-1})h^{-1} = gPg^{-1} \ \forall h \in P$, and so $g^{-1}Pg$ fixes P, as $(g^{-1}hg)P(g^{-1}hg)^{-1} = g^{-1}hgPg^{-1}h^{-1}g = gg^{-1}Pg^{-1}g = P$.
$\forall h \in P$

Therefore $g^{-1}Pg \subset N$.



Now, $\pi(g^{-1}Pg)$ has order dividing $|g^{-1}Pg|$ (as π is a homomorphism) so must have $|\pi(g^{-1}Pg)| = 1$ as $p \nmid |N/P|$ i.e. $g^{-1}Pg \subset P$. Hence $g^{-1}Pg = P$.

ii) Let Q be a Sylow-p-subgroup of G. We would like Q, P conjugate. We have Q acting on X (with orbit sizes $1, p, p^2, \dots$).

But $|X| \not\equiv 0 \pmod p$, so $\exists$ an orbit of size 1: say Q fixes gPg^{-1}. Thus $g^{-1}Qg$ fixes P (as before) so $g^{-1}Qg \subset N$.

Hence, $\pi(g^{-1}Qg) = \{e\}$ (as before) and so $g^{-1}Qg \subset P$, and $g^{-1}Qg = P$.

iii) We know that $n_p = |X|$ (by (ii)) and $|X| \equiv 1 \pmod p$, so $n_p \equiv 1 \pmod p$. Also, $n_p \mid |G|$ as n_p is an orbit of G, and $(n_p, p) = 1$, so we must have $n_p \mid m$.

Remarks

1. It is <u>not</u> true that $d \mid |G| \Rightarrow G$ has a subgroup of size d.

e.g. A_4 has no subgroup of order 6 (direct check)

<u>OR</u> We are about to show that A_5 is simple, so A_5 has no subgroup of order 30 (as a subgroup of index 2 would be normal.)

<u>OR</u> There is no subgroup of order 15 in S_5 (since there is no element of order 15).

2. Corollary 10 is the best possible. If $p < q$ are primes with $q \equiv 1 \pmod p$ then $\exists$ a non-cyclic (even non-Abelian) group of order pq

Warnings (about identifying a group)

1. If G has a normal subgroup H, we need not have $G \cong H \times G/H$
e.g. $\mathbb{Z}_4 \rhd \{0, 2\}$, but $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$

2. We can know H and G/H but not know G.
e.g. $G = \mathbb{Z}_4$, $H \cong \mathbb{Z}_2$, $G/H \cong \mathbb{Z}_2$, but $\mathbb{Z}_2 \times \mathbb{Z}_2$ also has $H \cong \mathbb{Z}_2$, $\frac{\mathbb{Z}_2 \times \mathbb{Z}_2}{H} \cong \mathbb{Z}_2$

3. If G has subgroups H, K, with $H \cap K = \{e\}$ and $|H||K| = |G|$ we need not have $G \cong H \times K$.

e.g. $G = S_3$, $H = \langle (1\,2) \rangle$, $K = \langle (1\,2\,3) \rangle$, but $S_3 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_3$ as S_3 is non-abelian while $\mathbb{Z}_2 \times \mathbb{Z}_3$ is abelian.

However, if H, K commute, then G IS $\cong H \times K$.
Define $\theta : H \times K \to G$, $(h, k) \mapsto hk$

$$(h,k)(h',k') = (hh',kk')$$

Then θ is a homomorphism, $\quad hkh'k' = hh'kk'$
due to commutativity.

θ is injective because $hk = e \Rightarrow h = k^{-1} \in H \cap K \Rightarrow h = k = e$
θ is surjective as $|G| = |H||K|$.

We say that G is the <u>internal direct product</u> of H and K

We know that if $H \leq G$, index 2, then H is normal. This is not true for a higher index, e.g. $\langle (1\ 2) \rangle$ in S_3. It is not even true if G is large e.g. $\langle (1\ 2) \rangle \times \mathbb{Z}_{1000}$ in $S_3 \times \mathbb{Z}_{1000}$. However:

<u>Theorem 11</u>

Let G be a group with a subgroup H of index k. Then, $|G| > k!$ $\Rightarrow G$ is not simple.

<u>Proof</u> (Very Important!)

Let H have left cosets $g_1H, g_2H, \ldots, g_kH$. G acts on H by left multiplication i.e. we have a homomorphism $\theta: G \to S_k$.
Then $\ker\theta$ is normal, so we are done, unless $\ker\theta = \{e\}$ or G

We cannot have $\ker\theta = \{e\}$ as $|G| > |S_k| = k!$, and we cannot have $\ker\theta = G$ (e.g. $g_2g_1^{-1}(g_1H) = g_2H \neq g_1H$) $\square$

e.g. $|G| = 48 \Rightarrow G$ not simple (as a Sylow-2-subgroup has order 16, index 3, and $48 > 3!$)

The techniques we have so far, such as Sylow, element-counting, and subgroups of small index, are enough to show that there is no simple group (apart from $\mathbb{Z}_p$, p prime) of order less than 60, which brings us to A_5.

Groups, Rings and Modules 7

Simplicity of A_n

A_4 is not simple, as it has a normal subgroup $V = \{e, (12)(34), (13)(24), (14)(23)\}$, which is normal as it is a union of conjugacy classes.

We aim to show that A_n is simple for $n \geq 5$.

Proposition 12

A_n is generated by its 3-cycles.

Proof:

For i, j, k distinct, $(i\,j)(j\,k) = (i\,j\,k)$
For i, j, k, l distinct, $(i\,j)(k\,l) = (i\,j)(j\,k)(j\,k)(k\,l) = (i\,j\,k)(j\,k\,l)$
Hence any product of an even number of transpositions is a product of 3-cycles.

Now, all 3 cycles are conjugate in A_n for $n \geq 5$. Hence, if H is normal in A_n, $(n \geq 5)$ and H contains any 3 cycle, then $H = A_n$ (as H must be the union of conjugacy classes).

Theorem 12

A_n simple $\forall n \geq 5$.

Proof:

By induction on n:

$n = 5$: Conjugacy classes in A_5 have sizes $\overset{e}{1}, \overset{(\cdot\cdot)(\cdot\cdot)}{15}, \overset{(\cdot\cdot\cdot)}{20}, 12, \overset{(\cdot\cdot\cdot\cdot\cdot)}{12}$ (sum $= 60$) and no sum of these, including 1, divides 60.

[Alternatively, suppose H is a proper normal subgroup of A_5. If $3 \mid |H|$, then by Cauchy, $\exists h \in H$, order 3, so H has a 3 cycle and $H = A_5$.

If $2 \mid |H|$, $\exists h \in H$ of order 2 by Cauchy. WLOG, $h = (12)(34) \in H$. Then also $(15)(34) \in H$, as they are conjugate and H is normal. Then the product $(12)(15) = (215) \in H$.

The only case left is $|H| = 5$. WLOG, $H = \langle (12345) \rangle$, not normal.

06/02/12

Groups, Rings and Modules (8)

Proof that A_n is simple $(n \geq 6)$

Given H normal in A_n, we have $A_{n-1} \subset A_n$ $\to \{\sigma \in A_n : \sigma(n) = n\}$

Claim $\exists \sigma \in H, \sigma \neq e, \sigma(n) = n$

Proof of Claim Choose $\sigma \in H, \sigma \neq e$. Say $\sigma(n) = i$ (WLOG $i \neq n$)

We seek $\sigma' \in H$, $\sigma' \neq \sigma$, $\sigma'(n) = i$. Then $\sigma^{-1}\sigma'(n) = n$.

Pick $j \neq i, n$, $\sigma(j) \neq j$ (as $\sigma \neq (i\ n)$) (we may have $\sigma(j) = n$, no effect

Now choose distinct $x, y \neq i, n, j, \sigma(j)$ $(n \geq 6)$

and let $\sigma' = (j\ x\ y)\,\sigma\,(j\ x\ y)^{-1}$

Then $\sigma' \in H$, $\sigma'(n) = i$, and $\sigma' \neq \sigma$ as ~~$\sigma(j) =$~~ $\sigma: j \mapsto \sigma(j)$, $\sigma': x \mapsto \sigma(j)$

So $H \cap A_{n-1} \neq \{e\}$. But $H \cap A_{n-1}$ is normal in A_{n-1} (as H is normal in A_n)

so $H \cap A_{n-1} = A_{n-1}$ (induction hypothesis)

Thus $(1\ 2\ 3) \in H$ $\square$

Finite Simple Groups as Building Blocks * NON-EXAMINABLE

Write $H \trianglelefteq G$, H normal in G.

For a finite group G, a *composition series* for G is a sequence

$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_k = \{e\}$ with each G_i/G_{i+1} simple.

(Equivalently, G_{i+1} is a *maximal* proper normal subgroup of G_i)

The G_i/G_{i+1} are the *composition factors* of G.

e.g. S_4 : $S_4 \triangleright A_4 \triangleright V \triangleright \{e, (12)(34)\} \triangleright \{e\}$

Factors: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$

$\mathbb{Z}_6$: $\mathbb{Z}_6 \triangleright \{0, 2, 4\} \triangleright \{0\}$ OR $\mathbb{Z}_6 \triangleright \{0, 3\} \triangleright \{0\}$

Factors: $\mathbb{Z}_2$, $\mathbb{Z}_3$; $\mathbb{Z}_3$, $\mathbb{Z}_2$

D_8 : $D_8 \triangleright \langle a \rangle \triangleright \{e, a^2\} \triangleright \{e\}$

Factors : $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_2$

OR D_8 : $D_8 \triangleright \{e, b, a^2, a^2b\} \triangleright \{e, b\} \triangleright \{e\}$

S_5 : $S_5 \triangleright A_5 \triangleright \{e\}$
Factors : $\mathbb{Z}_2 \quad A_5$

Clearly, every finite group has a composition series.

Jordan-Hölder Theorem : The factors are unique (up to re-ordering)

We say G is soluble if all factors G_i/G_{i+1} are cyclic.

$\Leftrightarrow$ "G is built out of cyclic groups"

$\Leftrightarrow$ "G is $G_0 \triangleright G_1 \triangleright \dots \triangleright G_k = \{e\}$ with all G_i/G_{i+1} abelian"

$\Leftrightarrow$ "G is built out of abelian groups." $\Leftrightarrow$ "G is nice" !!

e.g. 1. Any abelian group
2. D_{2n}
3. S_4
4. Not S_n $(n \geq 5)$

If $H \trianglelefteq G$, G soluble $\Leftrightarrow$ H, G/H soluble

So for example, any p-group is soluble (as $Z \neq \{e\}$)

Burnside's $p^\alpha q^\beta$ Theorem p, q primes, $|G| = p^\alpha q^\beta \Rightarrow G$ soluble

The Non-Abelian Finite Simple Groups

We have $\mathbb{Z}_p$ (p prime) and A_n $(n \geq 5)$. The next simple group has order 168 : $GL_3(\mathbb{Z}_2)$ - 3×3 invertible matrices, entries in the field $\mathbb{Z}_2$ and similarly, $GL_n(\mathbb{Z}_2)$, $\forall n \geq 3$.

What about $GL_n(\mathbb{Z}_p)$, (p prime)?

No, as det is a homomorphism with non-trivial kernel.

so try $SL_n(\mathbb{Z}_p) = \{A \in GL_n(\mathbb{Z}_p) : \det A = 1\}$

but this might have a centre $Z = \{\lambda I, \lambda^n = 1\}$

So we try $PSL_n(\mathbb{Z}_p) = SL_n(\mathbb{Z}_p)/Z$. These are simple (except for $n=2, p=2$, and $n=2, p=3$).

06/02/12 Groups, Rings and Modules ②

In total, we get 16 such infinite classes, 'Simple groups of Lie type', analogues of some continuous matrix groups.

<u>Classification Theorem</u> for finite simple groups

All the finite simple groups are:

1. $\mathbb{Z}_p$ (p prime) 2. A_n ($n \geq 5$)
3. The 16 infinite families of groups of Lie type
4. The 26 sporadic simple groups, ranging in size from 7920 (M_{11}, one of the Mathieu groups) to $\approx 10^{54}$, ($\mathbb{M}$, the monster)

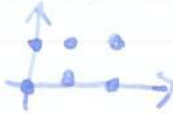
**

Chapter 2 : Rings

A ring is a set R, with binary operations $+$ and $\cdot$, and elements 0, 1 such that

1) Under $+$, R is an abelian group with identity 0
2) $\cdot$ is commutative, associative and distributive over $+$
   $\forall x, y, z \in R$, $xy = yx$, $x(yz) = (xy)z$, $x(y+z) = (xy)+(xz)$
3) $1x = x \;\; \forall x \in R$

Examples

1) $\mathbb{Z}$ (usual $+$ and $\cdot$)
2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
3) $\mathbb{Z}_n$ (any n)
4) $\mathbb{R}[X]$ - the set of polynomials with real coefficients
5) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ (this is a dense subset of $\mathbb{R}$)
6) $\mathbb{Z}(i) = \{a + bi \mid a, b \in \mathbb{Z}\}$  $\mathbb{C}$, "integer grid" in $\mathbb{C}$
7) All functions from $\mathbb{R}$ to $\mathbb{R}$ with pointwise operations
   e.g. $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$
   0 is the constant function 0, 1 is the constant function 1.
8) $C[0,1] = \{\text{continuous functions } [0,1] \to \mathbb{R}\}$
9) For any set X, we can make $\mathcal{P}(X)$ into a ring by
   

   $A + B = A \triangle B \; (= A \setminus B \cup B \setminus A)$, $A \cdot B = A \cap B$
   The 0 is $\emptyset$, and the 1 is X.
10) The 'trivial ring' $R = \{0\}$ (with $1 = 0$), unimportant

Our rings are "commutative, with 1", so for example
$M_n(\mathbb{R}) = n \times n$ real matrices are not a ring.

Remarks

1) We can write $0, 1$ as 0_R and 1_R

2) We have $0x = 0 \ \forall x \in R$ because $0x = (0+0)x = 0x + 0x$
$\Rightarrow 0x = 0$ (Group under $+$)

3) We have $(-x)y = -(xy) \ \forall x, y \in R$ because:
$(-x)y + xy = (-x+x)y = 0y = 0 \Rightarrow (-x)y = -(xy)$

We say $x \in R$ is invertible, or a unit, if $\exists y$ with $xy = 1$

e.g. in $\mathbb{Z}$: units are $1, -1$, in $\mathbb{Q}$; every $x \neq 0$ is a unit

In $\mathbb{Z}(i)$: units are $\pm 1, \pm i$

Note If y does exist, it is unique.

$x(y-y') = 0$

$xy(y-y') = y - y' = 0$

Suppose $xy' = 1$. Then $xy = xy'$ so ~~$yy = \dots$~~ $\Rightarrow y = y'$

Write y as x^{-1}.

Same as saying R is non trivial

A field is a ring R in which every $x \neq 0$ is invertible (and $0 \neq 1$)

e.g. $\mathbb{Z}$ is not a field, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields

$\mathbb{Z}_p$ (p prime) is a field, but not $\mathbb{Z}_n$ for composite n.

New Rings from Old

Sub-Rings

A subset S of a ring R is a sub-ring if it too is a ring under the same operations and constants.

So $S \subset R$ is a sub-ring $\Leftrightarrow$

i) S is a subgroup of R under $+$

ii) $x, y \in S \Rightarrow xy \in S$

iii) $1 \in S$

Groups, Rings and Modules (9)

e.g. in $\mathbb{Q}$, $\mathbb{Z}$ is a sub-ring.

In $\mathbb{Q}$: The dyadic rationals form a sub-ring $= \{ \frac{a}{2^b} \mid a \in \mathbb{Z}, b \in \mathbb{N}_0 \}$

It is the sub-ring "generated by $\frac{1}{2}$"

In $\mathbb{R}[X]$, the constants form a sub-ring.

In $\mathbb{Z}$, $2\mathbb{Z}$ is NOT a sub-ring $(1 \notin 2\mathbb{Z})$, and 0 is not a sub-ring. $(1 \notin \{0\})$

In fact, the only sub-ring of $\mathbb{Z}$ is $\mathbb{Z}$ itself because $1 \in S$, S a subgroup $\Rightarrow S = \mathbb{Z}$.

Direct Sums

For rings, R and S, we have a <u>direct sum</u> $R \oplus S$ defined on $R \times S$ with pointwise operations, $(x, y) + (x', y') = (x + x', y + y')$ and $(x, y)(x', y') = (xx', yy')$

The 0 is $(0_R, 0_S)$, and the 1 is $(1_R, 1_S)$

e.g. $\mathbb{Z} \oplus \mathbb{Z}$ is just the usual $\mathbb{Z}^2$.

<u>Warning</u>: R, S fields $\Rightarrow R \oplus S$ <u>not</u> a field

e.g. $(1, 0)$ NOT a unit

10/02/12 Groups, Rings and Modules (10)

Polynomial Rings

Given a ring, we can form $R[X]$, the "polynomials with coefficients in R" as follows:

$R[X] = \{ (a_0, a_1, a_2, \dots) : a_i \in R\ \forall i,\ a_i = 0\ \forall i \geq n, \text{ for some } n \}$

We can write $(a_0, a_1, \dots, a_{n-1})$ as $a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$

The greatest d with $a_d \neq 0$ is the <u>degree</u> of the polynomial, except for $0 = (0, 0, \dots)$ which does not have a degree.

$R[X]$ is a ring, with

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{2n} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$$ ← Using $x^i \times x^j = x^{i+j}$

$0 = (0, 0, \dots)$, $1 = (1, 0, \dots)$

We can view R as a subring of $R[X]$ by identifying it with the constants: $r \leftrightarrow (r, 0, 0, \dots)$

Given $f \in R[X]$, we have an induced function $\bar{f} : R \to R$, $x \mapsto \sum_{i=0}^{n} a_i x^i$ (where $f = \sum_{i=0}^{n} a_i X^i$)

e.g. In $\mathbb{R}[X]$, X^3 induces a function $x \mapsto x^3$ from $\mathbb{R}$ to $\mathbb{R}$

<u>Warning!</u> In $\mathbb{Z}_2[X]$, let $f = X^2 + X$. Then $f \neq 0$ ($\deg f = 2$)

But $\bar{f} = 0$ (as $x^2 + x = 0\ \forall x \in \mathbb{Z}_2$)

Let $f \in R[X]$, say $f = \sum_{i=0}^{n} a_i X^i$ with $a_n \neq 0$. We say f is <u>monic</u> if $a_n = 1$.

<u>Proposition 1</u> (Division Algorithm for polynomials)

Let $f, g \in R[X]$, with g monic. Then we can write $f = qg + r$ for some $q, r \in R[X]$ with $\deg r < \deg g$ (or $r = 0$)

Example

In $\mathbb{Z}[X]$, write X^3+X^2+1 as $q(X^2-3)+r$:

We have $X^3+X^2+1 = X(X^2-3)+X^2+3X+1$

$$= X(X^2-3)+1(X^2-3)+3X+4$$

$$= (X+1)(X^2-3)+3X+4$$

Note (on monic) : CANNOT write X^3+X^2+1 as $q(2X^2-3)+r$ ($\deg r < 2$) failing because 2 is not invertible in $\mathbb{Z}$

Proof (by induction on $\deg f$)

$\deg f < n = \deg g \Rightarrow f = 0\cdot g + f$

Given $\deg f = m \geq n$, say $f = \sum_{i=0}^{m} a_i X^i$.

inductive step

Then $f - a_m X^{m-n} g$ has degree $< m$, so $f - a_n X^{m-n} g = q g + r$

i.e. $f = (q + a_n X^{m-n})g + r$ $\square$

Homomorphisms, Ideals and Quotients

Let R and S be rings. A function $\theta : R \to S$ is a homomorphism if it preserves the ring structure.

i.e. θ is a group homomorphism from $(R,+)$ to $(S,+)$, and

$\theta(xy) = \theta(x)\theta(y)$ $\forall x,y \in R$, and $\theta(1_R) = 1_S$

Equivalently, θ is a homomorphism

$$\Leftrightarrow \theta(x+y) = \theta(x)+\theta(y),\ \theta(xy) = \theta(x)\theta(y),\ \theta(1) = 1 \quad \forall x,y \in R$$

If θ is also bijective, we say θ is an isomorphism and that R, S are isomorphic, written $R \cong S$.

10/02/12 Groups, Rings and Modules ⑩

Examples

1. $\theta : \mathbb{Z} \to \mathbb{Z}_3$, $x \mapsto x \pmod 3$

2. $\theta : \mathbb{Z}[X] \to \mathbb{C}$ "put $X = i$", $\sum_{j=0}^{n} a_n X^n \mapsto \sum_{j=0}^{n} a_n i^j$

Similarly, for any $\alpha \in \mathbb{C}$ we have a homomorphism $\mathbb{Z}[X] \to \mathbb{C}$ $\sum_{n=0}^{k} a_n X^n \mapsto \sum_{n=0}^{k} a_n \alpha^n$ called "evaluation at α"

3. $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Define $\theta : \mathbb{Z}_6 \to \mathbb{Z}_2 \oplus \mathbb{Z}_3$, $x \mapsto (x \pmod 3, x \pmod 2)$

This is well defined, a homomorphism, injective, and so bijective (both sides have size 6).

The image of θ is $\mathrm{Im}(\theta) = \theta(R) = \{\theta(r) : r \in R\}$

e.g. in example 2, $\mathrm{Im}(\theta) = \mathbb{Z}[i]$. The image is always a sub-ring of S. It is certainly a subgroup and $\theta(x)\theta(y) = \theta(xy)$ (So $\mathrm{Im}(\theta)$ is closed under $\cdot$) $\theta(1_R) = 1_S$ (So $1_S \in \mathrm{Im}(\theta)$)

$F(\mathbb{Y}) = F[\mathbb{Y}]$ The kernel of θ is $\ker\theta = \{r \in R : \theta(r) = 0\}$

e.g. in example 1, $\ker\theta = \{x \in \mathbb{Z}, x \equiv 0 \pmod 3\} = 3\mathbb{Z}$

This is not a sub-ring of $\mathbb{Z}$.

[In fact if $\ker\theta$ is a sub-ring, then $1 \in \ker\theta$ so $\forall r \in R$, $\theta(r) = \theta(r)\theta(1) = 0$, so θ is the zero-map, which is not a homomorphism unless S is trivial, $0 = 1$]

That motivates the following definition:

A subset $I \subseteq R$ is called an ideal if it is a subgroup of $(R, +)$ and $\forall x \in I$, $\forall r \in R$, $xr \in I$.

Thus, I an ideal $\Leftrightarrow$ $0 \in I$, $x, y \in I \Rightarrow x + y \in I$

$x \in I, r \in R \Rightarrow xr \in I$ $\leftarrow$ So no need for $x \in I \Rightarrow -x \in I$ as $-x = (-1)x$

Example

1. $3\mathbb{Z} \subset \mathbb{Z}$. Similarly, for any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal.

2. In $\mathbb{Z}[X]$, the set $\{(1+x^2)f : f \in \mathbb{Z}[X]\}$ is an ideal.

Digression Is this $\ker\theta$ for θ in example 2? ("Put $X = x$")

Certainly if g is of the form $(1+x^2)f$ then $\theta(g) = 0$.

$\theta(g) = \theta(1+x^2)\theta(f) = (1+x^2)\theta(f) = 0$

Conversely, given $g \in \ker\theta$, write $g = q_1(1+x^2) + r$ for some $q_1, r \in \mathbb{Z}[x]$ with r of the form $aX+b$ (by the division algorithm)

So we must have $\theta(ax+b) = 0$ i.e. $ai + b = 0 \Rightarrow a = b = 0$

3. In any ring, we have ideals $\{0\}$ and R. We say ideal I is proper if $I \neq R$. I is proper $\Leftrightarrow 1 \notin I$ (If $1 \in I$, then $\forall r$, $1 \cdot r \in I \Rightarrow I = R$.

4. In $\mathbb{Q}$, the only ideals are $\{0\}$ and $\mathbb{Q}$

(If $q \in I$, for some $q \neq 0$, then also $q^{-1}q = 1 \in I \Rightarrow I = \mathbb{Q}$]

[This is the same for any field]

Let $r \in R$. The set $(r) = rR = \{rx : x \in R\}$ is called the ideal generated by r; it is the smallest ideal containing r.

An ideal is principal "nice" if $I = (r)$ for some r.

Proposition 2

Every ideal of $\mathbb{Z}$ is principle ($= (n)$ for some $n \in \mathbb{Z}$)

Proof

WLOG $I \neq \{0\}$ ($\{0\} = (0)$)

Let n be the least positive element of I.

We claim that $I = (n)$

Proof of claim:

If $m \in (n)$ then $m \in I$ (as I is an ideal)

Conversely, given $m \in I$, $m = qn + r$, for some $0 \leq r < n$

Then $r \in I$ (as $r = m - qn$) $\Rightarrow r = 0$ (choice of n)

i.e. $m \in (n)$. $\square$

Similarly, given $r, s \in I$, write $(r, s) = rR + sR = \{rx + sy \mid x, y \in R\}$

This is the smallest ideal containing r and s, and we say that it is generated by r and s.

Examples / Warnings

1. In $\mathbb{Z}[X]$, we have ideal (X) = All polynomials with no constant term
   and ideal (2) = All polynomials with even coefficients
2. In $\mathbb{Z}[X]$, we also have an ideal $(2, X)$ = All polynomials with constant even coefficients

   It is ~~not~~ a principal ideal.

   Indeed, suppose $(2, X) = (f)$ for some $f \in \mathbb{Z}[X]$

   Then 2 is a multiple of f, so $f = \pm 1, \pm 2$, and

   X is a multiple of f, so $f = \pm 1, \pm X$.

   So $f = \pm 1$, which is not in $(2, X)$ ※
3. Similarly, in $\mathbb{Q}[X, Y] = (\mathbb{Q}[X])[Y]$

   We have ideal (X, Y) = All polynomials with no constant term.

   This is not principal, as if $(X, Y) = (f)$, then

   X is a multiple of f, so f = constant or constant $\times X$

   and similarly for Y, so f = constant $\notin (X, Y)$ ※

13/02/12 Groups, Rings and Modules (11)

$A+B = A \Delta B$, $A \cdot B = A \cap B$

4. Even worse, in $\mathcal{P}(\mathbb{N})$, we have ideal

$I = \{ A \in \mathcal{P}(\mathbb{N}) : A \text{ is finite} \}$

Then I is not even finitely generated.

Indeed, suppose $I = (A_1 \ldots A_n)$

Then $(A_1 \ldots A_n) \subset A_1 \cup A_2 \cup \ldots \cup A_n$

but $\exists A$, finite with $A \not\subset A_1 \cup \ldots \cup A_n$ ※

Given these examples, it is reassuring to have:

Theorem 3

Let F be a field. Then all ideals of $F[X]$ are principle.

Note Proof is the same as for $\mathbb{Z}$

Proof

Given ideal I in $F[X]$, WLOG $I \neq \{0\}$ ($\{0\} = (0)$)

Choose $f \in I$ with $\deg f$ minimal, WLOG, f is monic, because if $f = \sum_{i=0}^{k} a_i X^i$, we look at $a_k^{-1} f$ instead.

Claim $I = (f)$

Proof of Claim Certainly if $g \in (f)$, then $g \in I$.

Conversely, given $g \in I$, write $g = q f + r$ where $\deg r < \deg f$, or $r = 0$.

Then $r = g - qf \in I \Rightarrow 0$, otherwise we contradict minimality

$\Rightarrow g \in (f)$ $\square$

3

We know that for any homomorphism $\theta: R \to S$, $\ker\theta$ is an ideal of R

($\ker\theta$ is a subgroup, and $r \in \ker\theta \Rightarrow \theta(rx) = \theta(r)\theta(x) = 0 \Rightarrow rx \in \ker\theta$)

Conversely; given an ideal I in a ring R, we have the quotient group R/I

Elements are of the form $x + I$, with $(x+I)+(y+I) = (x+y)+I$

Define $\cdot$ on R/I by $(x+I)\cdot(y+I) = xy + I$

<u>Note</u> This is well defined: We need that if $x + I = x' + I$ and

$y + I = y' + I$, then $xy + I = x'y' + I$

Equivalently, $x - x' \in I$, $y - y' \in I$ and we want $xy - x'y' \in I$

But $xy - x'y' = (x-x')y + x'(y-y') \in I$

We can view this a motivating our definition for ideal

Then R/I <u>is</u> a ring (inherited from R)

e.g. $(x+I)(y+I) = (y+I)(x+I)$ because $xy = yx$

The 1 is $1 + I$: $(x+I)(1+I) = x + I$

We have $\pi : R \to R/I$, $x \mapsto x + I$ being a homomorphism with kernel I.

Thus

<u>Proposition 4</u> Let R be a ring, $I \subset R$. Then I is an ideal

$\Leftrightarrow \exists\, \theta$ a homomorphism, $\theta: R \to S$ with $\ker\theta = I$

<u>Proof:</u>

$(\Rightarrow)$ $\ker\theta$ is always an ideal.

$(\Leftarrow)$ Given an ideal I, look at the projection map $\pi : R \to R/I$ $\square$

15/02/12

Groups, Rings and Modules (12)

View R/I as "R, with x and y the same if $x-y \in I$",

i.e. "R, but with I set to zero"

e.g. $\mathbb{Z}[x]/\langle 1+x^2 \rangle$: Elements of the form $aX+b+\langle X^2+1\rangle$ $(a,b\in\mathbb{Z})$

So view $\frac{\mathbb{Z}[x]}{(1+x^2)}$ as polys of the form $aX+b$, which we add in the usual way, and multiply in the usual way except that $1+X^2=0$

Thus $2+3X+(1+X^2)+3+4X+(1+X^2) = 5+7X+(1+X^2)$

and $(2+3X+(1+X^2))(3+4X+(1+X^2)) = (2+3X)(3+4X)+(1+X^2)$

$$= 6+17X+12X^2+(1+X^2) = -6+17X+(1+X^2)$$

It looks as though $\frac{\mathbb{Z}[x]}{(1+x^2)} \cong \mathbb{Z}[i]$

<u>Theorem 5</u> (Isomorphism Theorem)

Let $\theta: R\to S$ be a ring homomorphism. Then $R/\ker\theta \cong \operatorname{Im}\theta$

<u>Proof</u>

The map $T: R/\ker\theta \to \operatorname{Im}\theta$, $r+\ker\theta \mapsto \theta(r)$ is a well defined group isomorphism (Isomorphism Theorem for groups).

Also, $T(rs+\ker\theta) = \theta(rs) = \theta(r)\theta(s) = T(r+\ker\theta)\,T(s+\ker\theta)$

i.e. $T((r+\ker\theta)(s+\ker\theta)) = T(r+\ker\theta)\,T(s+\ker\theta)$

and $T(1+\ker\theta) = \theta(1) = 1$

Thus, T is a ring isomorphism. $\square$

<u>Example</u> We have $\theta: \mathbb{Z}[X]\to\mathbb{C}$, $f\mapsto f(i)$

with $\operatorname{Im}\theta = \mathbb{Z}[i]$ and $\ker\theta = (1+X^2)$, so $\frac{\mathbb{Z}[X]}{(1+X^2)} \cong \mathbb{Z}[i]$

A proper ideal I in a ring R is <u>maximal</u> if there is no ideal J with $I \subsetneq J \subsetneq R$ (i.e. $I\subset J\subset R \Rightarrow J=I$ or $J=R$)

R

Examples

1. In $\mathbb{Z}$, n composite $\Rightarrow (n)$ not maximal (e.g. $(6) \subsetneq (2)$)
2. In $\mathbb{Z}$, p prime $\Rightarrow (p)$ is maximal

Indeed, suppose $(p) \subsetneq (n) \subsetneq \mathbb{Z}$ (valid because all ideals of $\mathbb{Z}$ are of this form)

So $n \mid p$, but $n \neq \pm p$ or ± 1 $\#$ as p is prime

3. In $\mathbb{Z}[X]$, the ideal (x) is NOT maximal (surprisingly?).

$(x) \subsetneq (2, x)$

No constant term — Even constant term

4. In $\mathbb{Z}[X]$, $(2, X)$ IS maximal.

Indeed, suppose ~~suppose~~ $(2,X) \subsetneq J$; so J has an element f with odd constant term. But then $f - 1 \in (2, x)$ (as the constant term is even) whence $1 \in J \Rightarrow J = \mathbb{Z}[x]$

5. In $\mathbb{Q}$, $\{0\}$ is maximal - the same for any field.
6. In fact, every proper ideal I in R is contained in a maximal ideal (Proof: Logic and Set Theory)

Maximal ideals are important because:

Theorem 6

Let I be a proper ideal in a ring R.
Then I maximal $\Leftrightarrow R/I$ is a field.

$\bigcirc \to \bigcirc$

$\pi : R \to R/I$

Proof

If R/I is not a field

We have $a \in R/I$, $a \neq 0$ but a is not invertible.

So (a) is a proper ideal in R/I

But then $J = \pi^{-1}((a))$ is an ideal in R with $I \subsetneq J \subsetneq R$

<u>If I is not maximal</u>

We have an ideal J with $I \subsetneq J \subsetneq R$

Choose $a \in J \setminus I$. Then in R/I, $a + I \neq 0$, but $a + I$ is not invertible. [If $(a+I)(b+I) = 1 + I$, then $ab - 1 \in I \underset{ab \in J,\ ab-1 \in J}{\Rightarrow} 1 \in J$ ※] $\square$

<u>Example</u>

Consider $\frac{\mathbb{Z}_3[X]}{(X^3 - X + 1)}$. Elements are $a + bX + cX^2 + (X^3 - X + 1)$, so there are 27 elements. Also, $(X^3 - X + 1)$ is maximal, because:

Suppose $(X^3 - X + 1) \subsetneq (f) \subsetneq \mathbb{Z}_3[X]$ for some f

(All ideals in $\mathbb{Z}_3[X]$ are of this form as $\mathbb{Z}_3$ is a field).

f is not cubic or constant (otherwise $(f) = (X^3 - X + 1)$ or $\mathbb{Z}_3[X]$)

So $X^3 - X + 1 =$ Linear $\cdot$ Quadratic, which is impossible as $X^3 - X + 1$ has no root.

<u>Conclusion</u> $\exists$ a finite field of size 27 $\Leftarrow$ Highly non-obvious.

17/02/12 Groups, Rings and Modules (13)

Integral Domains

A ring R is an integral domain if $ab = 0 \Rightarrow a = 0$ or $b = 0$ (and $0 \neq 1$)

i.e. "R has no zero-divisors"

e.g. $\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Q}$ (any field: if $a \neq 0$, $ab = 0$ then $a^{-1}ab = 0 \Rightarrow b = 0$)

$\mathbb{Z}_p$ (p prime) but NOT $\mathbb{Z}_n$ (n composite) ($\mathbb{Z}_6$: $2 \cdot 3 \equiv 0$)

Notes

1. In an integral domain we can 'cancel' a non-zero multiplier

i.e. $ab = ac$, $a \neq 0$, $a \cdot (b - c) = 0 \Rightarrow b = c$

2. If R is an integral domain, and $f, g \in R[X]$ with $\deg f = r$, $\deg g = s$, then ~~deg~~ $\deg(fg) = r + s$ (leading terms don't cancel)

[In $\mathbb{Z}_6[X]$, $(3X^2 + 2X + 1)(2X + 1)$ is not cubic]

3. A homomorphic image of an integral domain may NOT be an integral domain, e.g. $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$

4. In any ring R, the characteristic of R written $\text{char}(R)$, is the least +ve integer m with $\overbrace{1 + 1 + \ldots + 1}^{m \text{ times}} = 0$. (If no such m exists we say that $\text{char}(R) = 0$)

e.g. $\text{Char}(\mathbb{Z}) = \text{Char}(\mathbb{Z}[X]) = \text{Char}(\mathbb{Q}) = 0$

$\text{Char}(\mathbb{Z}_n) = \text{Char}(\mathbb{Z}_n[X]) = n$

If R is an integral domain, then $\text{char}(R)$ cannot be composite, as if $n = ab$, then $(\overbrace{1 + \ldots + 1}^{n \text{ times}}) = 0 = (\overbrace{1 + 1 + \ldots + 1}^{a \text{ times}}) \cdot (\overbrace{1 + \ldots + 1}^{b \text{ times}})$

So, in an integral domain, the subring generated by 1 is isomorphic to $\mathbb{Z}_p$ (p prime) or $\mathbb{Z}$.

Proposition 7 Every finite integral domain is a field.

Proof Given $a \in R$, $a \neq 0$, we seek $b \in R$ with $ab = 1$

The map $f: R \to R$, $x \mapsto ax$ is injective (as $ax = ay \Rightarrow x - y = 0$, $x = y$.)

Hence, f is surjective (as R is finite) so $\exists x$ with $ax = 1$ $\square$

Fields of fractions

Given a ring R, how do we "make it a field"?

We could quotient by the maximal ideal to get R/I (e.g. $\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}_7$

OR we could try to extend e.g. $\mathbb{Z} \to \mathbb{Q}$

Theorem 8

Let R be an integral domain. Then, $\exists$ a field F containing R.

(i.e. F has a sub-ring isomorphic to R)

Remarks

1. If R is not an integral domain, trivially, we cannot extend R to a field (as $\exists\, a, b \neq 0$ with $ab = 0$)
2. For $\mathbb{Z}$, take $\mathbb{Q}$ = Things of the form $\frac{a}{b}$, which contains a copy of $\mathbb{Z}$ via $n \mapsto \frac{n}{1}$

Proof

Define an equivalence relation $\sim$ on $\{(a, b) \mid a, b \in R, b \neq 0\}$ by $(a, b) \sim (c, d)$ if $ad = bc$

[This is an equivalence relation: Given $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$ we would like $(a, b) \sim (e, f)$. Given $ad = bc$, $cf = de$, we want $af = be$

17/02/12 Groups, Rings and Modules (3)

Multiplying: $adcf = bcde$ - now cancel cd (this is ok if $c \neq 0$, as R is an integral domain, whereas if $c = 0$, then $a = 0$ and $e = 0$)

Write F for the set of equivalence classes; write $\frac{a}{b}$ for $[(a,b)]$

Define $+$ on F by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

(Well defined, as $\frac{a}{b} = \frac{a'}{b'} \Rightarrow \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c}{d}$.

Indeed, given $ab' = ba'$, we want $\frac{ad+bc}{bd} = \frac{a'd+b'c}{b'd}$ i.e. $bd(a'd+b'c) = b'd(ad+bc)$)

Define $\cdot$ on F by $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

(Well defined, as $\frac{a}{b} = \frac{a'}{b'} \Rightarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$

Indeed, given $a'b = ab'$ we want $\frac{ac}{bd} = \frac{a'c}{b'd}$ i.e. $acb'd = a'cbd$)

Ring structure inherited from R e.g. $\frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b}$ as $\frac{ac}{bd} = \frac{ca}{db}$

The 0 is $\frac{0}{1}$ and the 1 is $\frac{1}{1}$.

F is a field as if $\frac{a}{b} \neq 0$, then $a \neq 0$, so $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1} = 1$

Finally, $\theta : R \to F$, $r \mapsto \frac{r}{1}$ is a homomorphism, and is injective:

$\frac{r}{1} = \frac{r'}{1} \Rightarrow r = r'$, so $\theta(R) \cong R$ □

<u>Prime Ideals</u>

A proper ideal I in a ring R is <u>prime</u> if $ab \in I \Rightarrow a \in I$ or $b \in I$

e.g. 1. In $\mathbb{Z}$, (p) is a prime <u>ideal</u> for prime <u>number</u> p

$(ab \in (p) \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b)$

2. In $\mathbb{Z}$, (n) is <u>not</u> prime if n is composite (e.g. $2 \cdot 3 \in (6)$ but $2, 3 \notin (6)$)

3. In $\mathbb{Z}[X]$, (X) is prime (f, g ~~do~~ have constant terms $\Rightarrow$ so does fg)

4. In a ring R, $\{0\}$ prime $\Leftrightarrow$ R is an integral domain

Proposition 9 Let I be an ideal in a ring R.

Then R/I an integral domain $\Leftrightarrow$ I is prime.

Proof

R/I not an integral domain $\Leftrightarrow \exists\, a+I,\ b+I \neq 0$ with $ab+I = 0$

$\Leftrightarrow \exists\, a, b$ with $a \notin I$, $b \notin I$, $ab \in I$ $\Leftrightarrow$ I is not prime $\square$

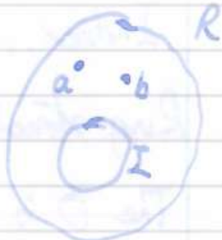
Corollary 10

Let I be an ideal in a ring R. Then I maximal $\Rightarrow$ I prime

Proof

R/I is a field $\Rightarrow$ R/I is an integral domain $\square$

OR directly:



If I is not prime, then $\exists\, a, b \notin I$ with $ab \in I$

so the ideal generated by I and a

(namely $(I, a) = I + aR$) must be the whole of R.

Hence $1 = i + ar$ for some $i \in I$, $r \in R$

Similarly, $1 = j + bs$, for some $j \in I$, $s \in R$

Multiply: $1 = \underset{\in I}{ij} + \underset{\in I}{abs} + \underset{\in I}{jar} + \underset{\in I \text{ as } ab \in I}{abrs} \quad \in I$

So $I = R$ $\#$

21/02/12 Groups, Rings and Modules 14

Factorisation

Euclidean Domain ⇐ Has division algorithm

$\Downarrow$ Trivial

Principal Ideal Domain ⇐ All ideals are maximal

$\Downarrow$ Heart of the section

Gauss' Lemma $\xrightarrow{\mathbb{Z}[x] \text{ is a}}$ Unique Factorisation Domain ⇐ Factorisation works

$\Downarrow$

Integral Domain

An integral domain is a principal ideal domain or PID if every ideal is principal ((r) for some r)

e.g. $\mathbb{Z}$, $F[x]$ (F any field)

NOT $\mathbb{Z}[X]$ as $(2, X)$ is not principal

An integral domain R is a Euclidean Domain if $\exists \varphi : R \setminus \{0\} \to \mathbb{N}_0$ such that 1. $\varphi(a) \leq \varphi(b)$ whenever $a | b$ (a divides b, i.e. $b = ac$ for some c)

Important One $\Rightarrow$ 2. $\forall a, b \in R$, $b \neq 0$, we can write $a = qb + r$ for some $q, r \in R$ with $\varphi(r) < \varphi(b)$ (or $r = 0$)

We say φ is a Euclidean Function for R.

Examples 1. $\mathbb{Z}$, with $\varphi(n) = |n|$

2. $F[x]$ (F any field) with $\varphi(f) = \deg f$

3. Silly example: any field with $\varphi(r) = 0 \ \forall r \neq 0$

Proposition 11 Every Euclidean Domain is a PID

Remarks

1. This is why we care about Euclidean Domains.
2. We've seen the proof twice already ($\mathbb{Z}$, $F[X]$)

Proof

Given an ideal I in R, $I \neq \{0\}$, choose $r \in I$ with $\varphi(r)$ minimal.

Claim $I = (r)$

Proof of Claim Certainly $(r) \subset I$ (as I an ideal)

Conversely, given $s \in I$, write $s = xr + y$, for some $x, y \in R$ with $\varphi(y) < \varphi(r)$ or $y = 0$
Then $y = s - xr \in I$, whence $y = 0$ (choice of r) $\square$

<u>Irrelevant Remark</u> $\exists$ PIDs that are not EDs (Examples are quite hard)

A more interesting example of a Euclidean Domain :

<u>Proposition 12</u> $\mathbb{Z}[i]$ is a Euclidean Domain
<u>Proof</u> For $z \in \mathbb{Z}[i]$, put $\varphi(z) = N(z) = |z|^2$ (the <u>Norm</u> of z)
Then φ multiplicative ($\varphi(z)\varphi(w) = \varphi(zw)\ \forall z, w$) so $z \mid w$
$\Rightarrow \varphi(z) \mid \varphi(w) \Rightarrow \varphi(z) \leq \varphi(w)$ $(z, w \neq 0)$

Given $z, w \in \mathbb{Z}[i]$, $w \neq 0$:
We ~~have~~ seek ~~that~~ $q, r \in \mathbb{Z}(i)$ with $z = qw + r$, $\varphi(r) < \varphi(w)$
i.e. $q \in \mathbb{Z}[i]$ with $\varphi(z - qw) < \varphi(w)$ ← we dared to go out from $\mathbb{Z}[i]$ to something bigger namely $\mathbb{C}$
$\Leftrightarrow |z - qw| < |w| \Leftrightarrow \left|\frac{z}{w} - q\right| < 1$
But for <u>any</u> $u \in \mathbb{C}$, $\exists q \in \mathbb{Z}[i]$ with $|u - q| < 1$. $\square$
(Just choose the closest q to u, i.e. choose $x \in \mathbb{Z}$ with $|x - \mathrm{Re}(u)| \leq \frac{1}{2}$ and $y \in \mathbb{Z}$ with $|y - \mathrm{Im}(u)| \leq \frac{1}{2}$, and then $|u - (x+iy)| \leq \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} = \frac{1}{\sqrt{2}}$)

Let R be an integral domain, and $r \in R$, with $r \neq 0$, r not a unit. We say that r is <u>irreducible</u> if $r = ab \Rightarrow a$ or b a unit.
e.g. in $\mathbb{Z}$, any prime p (or $-p$)
In $\mathbb{Z}[X]$, X is irreducible, X^2+1 is irreducible (no linear factor)
In $\mathbb{Z}_3[X]$, $X^3 - X + 1$ irreducible (or else = linear × quadratic, but it has no roots)
We say a, b (in an integral domain R) are associates, if $a = bc$ for some unit c.
e.g. $5, -5$ in $\mathbb{Z}$
$3+4i$, $i(3+4i)$ in $\mathbb{Z}[i]$

21/02/12

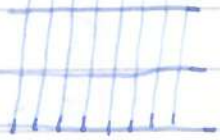
Equivalently, $a|b$ and $b|a$.
(Indeed, if a, b are associates, then $a|b$, $b|a$. Conversely, if $a = cb$, $b = da$, then $a = cda$ whence $cd = 1$ i.e. c a unit, unless $a = 0$ but then $b = 0$)

Equivalently, $(a) = (b)$ $\Leftarrow a|b, b|a$

An integral domain R is a Unique Factorisation Domain (UFD) if it satisfies
(UFD1): For $r \in R$, $r \neq 0$, not a unit $\Rightarrow$ We can write r as a product of irreducibles (i.e. $r = a_1 \dots a_k$ for some $a_1 \dots a_k$ irreducible)
(UFD2): This is unique, up to reordering and multiplying by units.
(i.e. if $a_1 \dots a_k = b_1 \dots b_l$, some irreducibles $a_1 \dots a_k, b_1 \dots b_l$, then $k = l$ and after reordering, a_i and b_i are associates $\forall i$).

Example $\mathbb{Z}$ (UFD1 was an easy induction. UFD2 was considerably harder: it rested on "$p|ab \Rightarrow p|a$ or $p|b$"

22/02/12



__Example__

$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ not a UFD

We have $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

In $R = \mathbb{Z}[\sqrt{-3}]$, the units are only ± 1 ($r \neq 0, \pm 1 \Rightarrow |r| > 1 \Rightarrow |\frac{1}{r}| < 1 \Rightarrow \frac{1}{r} \notin R$)

So $1 \pm \sqrt{-3}$ are certainly not associates of 2.

We just need to check that $2, 1 \pm \sqrt{-3}$ are irreducible.

2: Suppose $ab = 2$ for some $a, b \in R$, non-units

So $N(a)N(b) = N(2) = 4$ (as N is multiplicative) often a useful step

But $N(a), N(b) \in \mathbb{Z}$ ($N(x + y\sqrt{-3}) = x^2 + 3y^2 \in \mathbb{Z}$)

So $N(a), N(b) \in \{1, 2, 4\}$. We cannot have $N(a) = 1$ (as then a is a unit, $a = \pm$

So $N(a) = N(b) = 2$. But this is impossible as $x^2 + 3y^2 = 2$ has no solutions with $x, y \in \mathbb{Z}$.

$1+\sqrt{-3}, 1-\sqrt{-3}$: $N(1+\sqrt{-3}) = N(1-\sqrt{-3}) = 4$, so the same argument applies

__Remarks__ 1. Or in $\mathbb{Z}[\sqrt{-5}]$: $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

2. Historically, many mathematicians were led astray by the fact that sub-rings of $\mathbb{C}$ may not be UFDs.

Let R be an integral domain, r a non-zero, non unit. We say that r is __prime__ if $r \mid ab \Rightarrow r \mid a$ or $r \mid b$

e.g. in $\mathbb{Z}$, any prime (in the usual sense) p or $-p$

Note that r prime $\Rightarrow$ r irreducible. Indeed, if $r = ab$, then $r \mid ab$. $\Rightarrow r \mid a$ or $r \mid b$. But $r \mid a \Rightarrow r, a$ associates (as $r \mid a$, $a \mid r$) $\Rightarrow b$ a unit

The converse is false: If $\mathbb{Z}[\sqrt{-3}]$, 2 is irreducible, but not prime, because $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$ while $2 \nmid 1 \pm \sqrt{-3}$ ($1 \pm \sqrt{-3}$ irreducible)

__Lemma 13__ Let R be an integral domain. Then R is a UFD

$\Leftrightarrow$ It satisfies UFD1 and

UFD2': All irreducibles are prime

__Proof__ ($\Leftarrow$) Suppose $r_1 \dots r_k = s_1 \dots s_l$, where all r_i, s_j are irreducible. Then r_1 prime, $r_1 \mid s_1 \dots s_l$

So $r_1 | s_j$ for some j, WLOG, $r_1 | s_1$. But s_1 is irreducible $\Rightarrow r_1$ is an associate of s_1 (r_1 not a unit). So WLOG, $r_1 = s_1$ (multiply one other r_i or s_j by a unit if necessary)
Hence $r_2 \dots r_k = s_2 \dots s_l$, and we are done by induction on $k+l$

($\Rightarrow$) Suppose r irreducible, but not prime. We say $r | ab$, $r \nmid a$, $r \nmid b$.
Write $rs = ab$. We have $a = r_1 \dots r_k$, $b = s_1 \dots s_l$, for some r_i, s_j irreducibles. Also have $s = t_1 \dots t_m$, all t_i irreducible.
But now $r\, t_1 \dots t_m = r_1 \dots r_k s_1 \dots s_l$ are _different_ factorisations (no r_i or s_j are associates of r, since $r \nmid a$, $r \nmid b$ #) □

Note that, for $r \neq 0$: (r) prime $\Leftrightarrow$ r prime
Indeed, r prime says $r | ab \Rightarrow r | a$ or $r | b$

$$ab \in (r) \quad a \in (r) \quad b \in (r)$$

[also, r non-unit $\Leftrightarrow$ (r) is proper]

Lemma 14 R a ~~UFD~~ PID, $r \in R$, $r \neq 0$. Then the following are equivalent:
(i) r irreducible
(ii) (r) prime $\leftarrow$ r is prime
(iii) (r) maximal

Proof
(ii) $\Rightarrow$ (i) : Primes are always irreducible in a ~~UFD~~ PID
(iii) $\Rightarrow$ (ii) : Maximal ideals are always prime.
(i) $\Rightarrow$ (iii) : (r) proper as r is a non-unit. Suppose $(r) \subsetneq J$, for some ideal J. We want $J = R$. We have $J = (x)$ for some x (as R is a PID). So $x | r$, $r \nmid x$ (as $r \in (x)$, $x \notin (r)$)
Thus x is a unit (r irreducible), so $J = R$.

Remark So in a PID, I maximal $\Leftrightarrow$ I is prime
(unless $I = \{0\}$, always prime, hardly ever maximal)

22/02/12

Groups, Rings and Modules

Lemma 15

R a PID, $r \in R$, non-zero, non-unit. Then r is a product of irreducibles. ~~Suppose not.~~

Proof

Suppose not, and r is not a product of irreducibles (bad)

Then r is not irreducible, so $r = a_1 b_1$ with a_1, b_1 non-units. So we must have a_1 or b_1 also bad (otherwise r is not bad). WLOG, a_1 is bad.

So $a_1 = a_2 b_2$, for some a_2, b_2 non-units, with say a_2 bad.

Continue on, to obtain $(r) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$

Then, let $I = \bigcup_{i=1}^{\infty} (a_i)$. This is an ideal, and

~~so~~ $I = (x)$ for some x, (as R is a PID).

Hence, $x \in (a_k)$ for some k.

But then, $(a_k) = I \Rightarrow (a_k) = (a_{k+1}) = \dots$ #

$\square$

24/02/12

Groups, Rings and Modules (16)

Theorem 16
Every PID is a UFD.

Proof UFD 1 (can factorise into irreducibles): Lemma 15
UFD 2 (irreducibles are prime): Lemma 14 $\square$

So we know $\mathbb{Q}[x]$ (or $F[x]$ for any field F) and $\mathbb{Z}[i]$ are UFDs.

Application: Sums of Two Squares

Which natural numbers are of the form x^2+y^2, $x, y \in \mathbb{Z}$?
$2 = 1^2+1^2$, 3 ✗, $5 = 2^2+1^2$, 7 ✗, 11 ✗, $13 = 3^2+2^2$, $17 = 4^2+1$
19: ✗ $\Leftarrow$ Cannot get any $n \equiv 3 \pmod 4$ since squares $\equiv 0$ or $1 \pmod 4$

Aim: Prime $p \equiv 1 \pmod 4 \Rightarrow p$ is a sum of two squares

Reminder For p an odd prime, -1 is a square in $\mathbb{Z}_p \Leftrightarrow p \equiv 1 \pmod 4$
because if $p = 4k+3$, in $\mathbb{Z}_p$, if $x^2 = -1$, then, $x^{4k+2} = (x^2)^{2k+1} = -1$
contradicting Fermat.
If $p = 4k+1$, $(4k)! = -1$ in $\mathbb{Z}_p$ (Wilson). But
$(4k)! \equiv (2k)!^2$ (we multiply by $(-1)^{\text{even}}$), so take $x = (2k)!$
So, for $p \equiv 1 \pmod 4$, $p \mid x^2+1$ for some x.
We want $p = x^2+y^2$ for some x.

Theorem 17 Let $p \equiv 1 \pmod 4$ be prime. Then p is a sum of two squares

Proof We have $x \in \mathbb{Z}$ with $p \mid x^2+1$, so in $\mathbb{Z}[i]$, $p \mid (x+i)(x-i)$
but $p \nmid (x+i), (x-i)$ (As $p(s+it) = ps+pti$)
So p is not prime (in $\mathbb{Z}[i]$). So p is not irreducible
(as $\mathbb{Z}[i]$ is a UFD). We write $p = a \cdot b$, with a, b non-units.
So $p^2 = N(p) = N(a)N(b)$
But $N(a), N(b) \neq 1$ (as a, b are not units), so $N(a) = p$, as required. $\square$

Where the work is.

Corollary 18 n is a sum of two squares $\Leftrightarrow$ In the prime factorisation of n, each prime $\equiv 3 \pmod 4$ occurs to an even power.

Proof
($\Leftarrow$) For p prime, $p \equiv 1 \pmod 4$, p is a sum of two squares.
$p = 2 = 1^2+1^2$. If $p \equiv 3 \pmod 4$, $p^2 = p^2+0^2$.

But r, s sums of two squares $\Rightarrow$ so is rs (as $N(ab) = N(a)N(b)$.

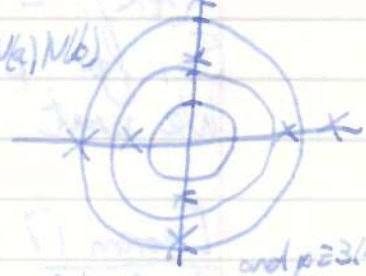
($\Rightarrow$) Let $n = x^2 + y^2$, $p \equiv 3 \pmod 4$ a prime with $p \mid n$.
We will show that x, y are multiples of p (whence $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$
In $\mathbb{Z}_p$, $x^2 + y^2 \equiv 0$, and so $x = y = 0$, (otherwise $(xy^{-1})^2 + 1 = 0$ contradicting -1 not a square in $\mathbb{Z}_p$) $\square$

e.g. $5 \cdot 13 \cdot 19^2$ __is__ a sum of two squares, but $5 \cdot 13 \cdot 19 \cdot 23$ is __not__.

We have seen that if $p \equiv 1 \pmod 4$ is prime in $\mathbb{Z}$, then p is __not__ irreducible (= prime) in $\mathbb{Z}[i]$. What are the irreducibles in $\mathbb{Z}[i]$?
(these are sometimes called the __complex primes__ or __Gaussian primes__)

__Theorem 19__ The irreducibles in $\mathbb{Z}[i]$ are precisely
i) All $r \in \mathbb{Z}[i]$ with $N(r)$ prime (in $\mathbb{Z}$)
ii) All primes p in $\mathbb{Z}$ with $p \equiv 3 \pmod 4$ (and their associates, $-p, ip, -ip$)

__Proof__
If $N(r)$ is prime: Suppose $r = ab$, then $N(r) = N(a)N(b)$
So $N(a)$ or $N(b) = 1$, i.e. a, or b a unit.
If p is prime in $\mathbb{Z}$ with $p \equiv 3 \pmod 4$, suppose $p = ab$. Then $p^2 = N(a)N(b)$. But we cannot have $N(a) = p$ (otherwise p would be a sum of two squares, and $p \equiv 3 \pmod 4$)



Conversely, let r be irreducible. If $N(r)$ is prime (in $\mathbb{Z}$) we have (i) case.
If $N(r) = p^2$, for some prime p, then $r\bar{r} = pp$. But $r, \bar{r}$ irreducible, so $r = p$ (up to a unit) as $\mathbb{Z}[i]$ is a UFD. Also, we must have $p \equiv 3 \pmod 4$ otherwise p is not irreducible.
If $N(r) \neq p, p^2$ for any prime p: $N(r) = ab$ where $1 < a < b < N(r)$
Thus $r\bar{r} = ab$, whence $r = a$, $\bar{r} = b$ or $r = b$, $\bar{r} = a$ (up to units) as $\mathbb{Z}[i]$ is a UFD. But a, b are not conjugates $\times$ $\square$

Note $r, \bar{r}$ are both, or neither irreducible in all cases

27/02/12

Groups, Rings and Modules (17)

Gauss' Lemma

Aim $f \in \mathbb{Z}[x]$ irreducible in $\mathbb{Z}[x] \Leftrightarrow$ irreducible in $\mathbb{Q}[x]$ (except silly cases, e.g. x^2+x+1 irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ (no linear factors) but $7(x^2+x+1)$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$)

Useful because

- Helpful for showing $\mathbb{Z}[x]$ is a UFD
- To show that polynomials are irreducible in $\mathbb{Q}[x]$ (and f irreducible in $\mathbb{Q}[x] \Rightarrow (f)$ maximal $\Rightarrow \frac{\mathbb{Q}[x]}{(f)}$ is a field)

HCFs

R an integral domain, $a, b \in R$. We say $c \in R$ is an HCF of a and b if:

i) $c \mid a$, $c \mid b$

ii) $d \mid a$, $d \mid b \Rightarrow d \mid c \quad \forall d \in R$.

If the HCF exists, it is unique (up to associates): If c, c' are HCFs then $c \mid c'$ and $c' \mid c$

e.g. in $\mathbb{Z}$, HCFs of 8, 10 are 2, -2.

In a UFD, HCFs do always exist.

Indeed, given $a \in R$, $a = r_1 \dots r_n$ ($r_1, \dots, r_n$ irreducibles), the factors of a are all products $\prod_{i \in I} r_i$ (and their associates) - we cannot have any other factor s as otherwise, $a = st$ would contradict the uniqueness of prime factorisation. Hence if $a = r_1 \dots r_k s_1 \dots s_l$, $b = r_1 \dots r_k t_1 \dots t_m$ (r_i, s_i, t_i irreducible, no s_i an associate of t_j) then the HCF of a and b is $r_1 \dots r_k$.

For R a UFD, we say $f \in R[x]$ is <u>primitive</u> if no non-unit divides all coefficients of f (i.e. HCF of coefficients is 1)

e.g. in $\mathbb{Z}[x]$, x^2+x+1 is, $2x^2+2x+1$ is not.

Theorem 20

Let $f \in \mathbb{Z}[x]$ be primitive. Then f irreducible in $\mathbb{Z}[x] \Leftrightarrow f$ irreducible in $\mathbb{Q}[x]$

Proof

($\Leftarrow$) If f is not irreducible in $\mathbb{Z}[x]$ then $f = gh$, for some $g, h \in \mathbb{Z}[x]$, non-constant (as f is primitive). But g, h are not units in $\mathbb{Q}[x]$ (as they are non constant), so f is not irreducible in $\mathbb{Q}[x]$

($\Rightarrow$) Given $f \in \mathbb{Z}[x]$, suppose $f = gh$ in $\mathbb{Q}[x]$, g, h non-units
We'll show that some rational multiples g' and h' of g and h have $g'h' = f$ and $g', h' \in \mathbb{Z}[x]$. Multiplying up, we have $nf = g'h'$ for some $n \in \mathbb{Z}$
and $g', h' \in \mathbb{Z}[x]$ (non constant). If n is a unit in $\mathbb{Z}$ (i.e. ± 1) we are done. If not, choose a prime p with $p \mid n$.
<u>Claim:</u> p divides all coefficients of g' or all coefficients of h'.
<u>Proof of Claim</u> Suppose not. Write $g' = \sum a_i X^i$, $h' = \sum b_i X^i$ and choose the least j with $p \nmid a_j$, and the least k with $p \nmid b_k$.
Then the X^{j+k} coefficient of $g'h'$ is not a multiple of p ※
Say $p \mid g'$. Then $\frac{n}{p} f = (\frac{1}{p} g') h'$ - done by induction on n (or on the number of prime factors of n). $\square$

<u>Remarks</u>
1. The key fact in the proof, namely "$p \mid fg \Rightarrow p \mid f$ or $p \mid g$" is sometimes also called Gauss' Lemma.
2. We can rephrase this key fact as $c(fg) = c(f)c(g)$ where $c(f)$ is called the <u>content</u> of f: the HCF of its coefficients.

<u>Theorem 20'</u> (Gauss' Lemma): R a UFD, with field of fractions F. Then a primitive $f \in R[X]$ is irreducible in $R[X]$ $\Leftrightarrow$ irreducible in $F[X]$

<u>Theorem 21</u>: $\mathbb{Z}[X]$ is a UFD
<u>Proof</u> Given $f \in \mathbb{Z}[X]$, write $f = ng$, where $n \in \mathbb{Z}$, g primitive.
Write $n = r_1 \dots r_k$, each r_i irreducible in $\mathbb{Z}$ ($\mathbb{Z}$ a UFD), so in $\mathbb{Z}[X]$.
If g irreducible in $\mathbb{Z}[X]$, we are done.
If not, write $g = hh'$, for some h, h' in $\mathbb{Z}[X]$ with $\deg h$, $\deg h' < \deg g$ (as g is primitive). But we can factorise h, h' (by induction on degree).
<u>Uniqueness</u>
Suppose $f = r_1 \dots r_k g_1 \dots g_l$ and $f = r_1' \dots r_m' g_1' \dots g_n'$ where the r_i, r_i' are irreducible in $\mathbb{Z}$ and the g_i, g_i' are primitive, and irreducible

Then $r_1 \dots r_k = r_1' \dots r_m'$ = HCF of coefficients of f, as a product of primitives is primitive.
So $r_1, \dots, r_k = r_1', \dots, r_n'$ in some order (multiplying by a unit if necessary) as $\mathbb{Z}$ is a UFD.
So $g_1 \cdots g_l = g_1' \dots g_n'$

But all the g_i, g_i' are irreducible in $\mathbb{Q}[X]$ by Theorem 20, so $g_1, \dots, g_l = g_1', \dots, g_m'$ in some order because $\mathbb{Q}[X]$ is a UFD.

Theorem 21'
R a UFD $\Rightarrow R[X]$ a UFD
Proof is the same.

Hence $\mathbb{Z}[X, Y] \overset{\mathbb{Z}[X][Y]}{=}$ or $\mathbb{Q}[X, Y] = \mathbb{Q}[X][Y]$ are UFDs.

29/02/12

<u>Proposition 22 (Eisenstein's Criterion)</u>

Let $f \in \mathbb{Z}[X]$ be primitive. Say $f = \sum_{i=0}^{k} a_i X^i$. Suppose $\exists$ a prime p with $p \mid a_0, p \mid a_1, \ldots, p \mid a_{k-1}$, $p \nmid a_k$ and $p^2 \nmid a_0$. Then f is irreducible.

e.g. $17X^4 + 3X^2 + 6$ irreducible $(p = 3)$

$X^n - p$ (p prime) irreducible (use p)

<u>Remarks</u>

1. Hence, f irreducible in $\mathbb{Q}[X]$ (Gauss' Lemma)
2. We do need $p^2 \nmid a_0$ e.g. $(X+2)^2 = X^2 + 4X + 4$

<u>Proof</u>

Suppose not. We have $f = gh$, with $g = \sum_{i=0}^{m} g_i X^i$, $h = \sum_{i=0}^{n} h_i X^i$ $(m, n < k)$. We have $a_0 = g_0 h_0$, so exactly one of g_0, h_0 is a multiple of p, say $p \mid g_0$

<u>CLAIM</u> $p \mid g_i \ \forall i \leq m$ (Then we're done: $p \mid g$ so $p \mid gh$ ※)

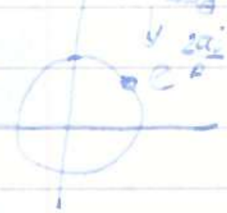
<u>Proof of Claim</u> For any $1 \leq i \leq m$: $a_i = g_i h_0 + \underbrace{g_{i-1} h_1 + \ldots + g_0 h_i}_{\text{multiple of } p \text{, by induction}}$

$p \mid a_i$, a_i is a multiple of p.

So $p \mid g_i h_0$, so $p \mid g_i$ (as $p \nmid h_0$) $\square$

<u>Example</u>

An irreducible polynomial satisfied by $e^{\frac{2\pi i}{p}}$, p prime?



Try $(X^p - 1)/(X-1) = X^{p-1} + X^{p-2} + \ldots + X + 1$

(a 'cyclotomic' polynomial)

"Put $X = Y + 1$": The above polynomial is irreducible

$\Leftrightarrow \frac{(Y+1)^p - 1}{Y}$ irreducible

i.e. $Y^{p-1} + \binom{p}{1} Y^{p-2} + \binom{p}{2} Y^{p-3} + \ldots + \binom{p}{p-2} Y + \binom{p}{p-1}$

This is irreducible by Eisenstein (using p).

<u>Two views of $\mathbb{Z}[\alpha]$</u>

Let $\alpha \in \mathbb{C}$. Write $\mathbb{Z}[\alpha]$ for the sub-ring of the complex numbers generated by $\mathbb{Z}$ and α: $\mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[X]\}$

$= \{\sum_{i=0}^{k} a_i \alpha^i$, where all $a_i \in \mathbb{Z}\}$

Recall that α is Algebraic if it is a root of a non-zero polynomial $f \in \mathbb{Z}[X]$. We say α is an <u>algebraic integer</u> if it is the root of a <u>monic</u> $f \in \mathbb{Z}[X]$. e.g.

7, $X - 7$ $\qquad$ $\sqrt{2}$, $X^2 - 2$ $\qquad$ $e^{\frac{2\pi i}{3}}$, $X^3 - 1$ (or $X^2 + X + 1$)

Let $\alpha \in \mathbb{C}$ be an algebraic integer: say α is the root of a monic $f \in \mathbb{Z}[x]$, $\deg f = n$.
Then $\mathbb{Z}[\alpha] = \{ \sum_{i=0}^{n-1} a_i \alpha^i : a_0, \dots, a_{n-1} \in \mathbb{Z} \}$ (division Algorithm)
e.g. $\mathbb{Z}[\alpha]$, α a root of x^2+2x+2, is $\{a + b\alpha, a, b \in \mathbb{Z}\}$
WLOG, f is irreducible: if $f = gh$ look at g or h instead.

Other Viewpoint We have a homomorphism $\theta : \mathbb{Z}[x] \to \mathbb{Z}[\alpha]$, $g \mapsto g(\alpha)$
This is surjective.
What is $\ker\theta$? Certainly, all multiples of f are in $\ker\theta$. We cannot have any other $g \in \ker\theta$. Indeed given such a g, $\deg g < n$
In $\mathbb{Q}[x]$: $\{ g : g(\alpha) = 0 \} \supsetneq f$. But (f) is maximal as f is irreducible. So $\{g : g(\alpha) = 0\} = \mathbb{Q}[x]$ ※
Thus $\mathbb{Z}[x]/(f) \cong \mathbb{Z}[\alpha]$
In conclusion Quotienting by (f) can be viewed as "adding in a root of f"

Nöetherian Rings

A ring R is Nöetherian if every ideal is finitely generated e.g any PID.
NOT $\mathcal{P}(\mathbb{N})$ - the ideal of finite sets is not finitely generated (f.g.)
NOT $\mathbb{Z}[x_1, x_2, x_3, \dots]$ - ideal $(x_1, x_2, \dots) = \{f$ with no constant term$\}$ - this is not finitely generated.

AIM
$\mathbb{Z}[x]$ Nöetherian (Ideals in $\mathbb{Z}[x]$ "aren't too bad")
We say that R has the ascending chain condition (ACC) if whenever we have ideals $I_1 \subset I_2 \subset I_3 \subset \dots$ then $I_n = I_{n+1} = \dots$ for some n.

Proposition 23
R is Nöetherian
$\Leftrightarrow$ R has an ACC

Proof ($\Rightarrow$)
Given $I_1 \subset I_2 \subset \dots$, let $I = I_1 \cup I_2 \cup \dots$
Then $I = (r_1, \dots, r_k)$ for some $r_1, \dots, r_k \in I$
We have $r_1 \in I_{n_1}, \dots r_k \in I_{n_k}$ for some $n_1, \dots, n_k$

So $r_1, \dots r_k \in I_n$ $(n = \max(n_1, \dots, n_k))$,
So $I_n = I$, i.e. $I_n = I_{n+1} = \dots$

($\Leftarrow$) Let I be an ideal of R, not finitely generated.
Choose $r_1 \in I$
Then $(r_1) \in I$ (as I not finitely generated)
So $\exists (r_2) \in I \setminus (r_1)$
Then $(r_1, r_2) \neq I$ (as I is not finitely generated)
Proceed by induction, to obtain,
$(r_1) \subsetneq (r_1, r_2) \subsetneq (r_1, r_2, r_3) \subsetneq \dots$ $\square$

Theorem 24 (Hilbert's Basis Theorem)
R Noetherian $\Rightarrow R[x]$ Noetherian

Proof
Let I be an ideal in $R[X]$. For $n = 0, 1, 2, \dots$, let I_n be
$I_n = \{r \in R \mid r$ is the leading coefficient of some $f \in I$ of degree $n\} \cup \{0\}$
$= \{r \in R : rX^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in I$, for some $a_{n-1}, \dots, a_0 \in R\}$
Each I_n is an ideal in R.
We have $I_0 \subset I_1 \subset I_2 \subset \dots$ (If $f \in I$, $\deg f = n$, then $Xf \in I$, $\deg(Xf) = n+1$)
So by ACC we have $I_N = I_{N+1} = \dots$ for some N.
For each $n \leq N$, we have $I_n = (r_n^{(1)}, r_n^{(2)}, \dots, r_n^{(k_n)})$, for some $r_n^{(i)} \in R$
For each $r_n^{(i)}$, choose $f_n^{(i)} \in I$ with $\deg f_n^{(i)} = n$, leading term $r_n^{(i)}$
CLAIM: $I = (f_n^{(i)} : n \leq N, i \leq k_i) \trianglelefteq J$
Proof of Claim: Certainly $J \subset I$.
Conversely, if $I \not\subset J$, then choose $g \in I \setminus J$ of minimal degree.
Say $\deg g = n$, with leading coefficient r.
__If $n \leq N$__
We have $r = \sum c_i r_n^{(i)}$, for some $c_1, \dots, c_{k_n} \in R$.
But then $g - \sum_i c_i f_n^{(i)} \in I$ and has degree $< n$, and does not belong to J (otherwise g does) $\#$
__If $n > N$__
We have $r \in I_n = I_N$, so we have $r = \sum_i c_i r_N^{(i)}$, for some $c_1, \dots c_{k_N} \in R$
But then, $g - (\sum c_i f_N^{(i)})X^{n-N} \in J$, and has degree $< n$, and does not belong to J (otherwise g does) $\#$ $\square$

__Examples__
1. $\mathbb{Z}[x]$ Noetherian
2. $\mathbb{C}[X, Y]$ (or $\mathbb{C}[X_1, \dots, X_n]$) Noetherian, as $\mathbb{C}[X]$ is – even though $\mathbb{C}[X, Y]$ is not a PID.

e.g. Let $f_i \in \mathbb{C}[X_1, \dots, X_n]$, $i \in I$, and let
$A = \{(z_1, \dots, z_n) \in \mathbb{C}^n : f(z_1, \dots, z_n) = 0 \ \forall i\}$ $\leftarrow$ where all the f_i vanish.
Then in fact A is equal to where a __finite__ set of polynomials vanish.

Chapter 3 : Modules

"A module is like a vector space, but over a ring" ← Not necessarily a field

Let R be a ring. An R-module is a set M with operations $+ : M \times M \to M$ and $\cdot : R \times M \to M$ such that

i) $(M, +)$ is an abelian group.

ii) $r(x+y) = rx + ry \quad \forall r \in R, x, y \in M$

iii) $r(sx) = (rs)x \quad \forall r, s \in R, x \in M$

iv) $1x = x \quad \forall x \in M$

V) $(r+s)x = rx + sx \quad \forall r, s \in R, x \in M$

Note that these are exactly the usual vector space axioms.

Examples

1. R any field, M any vector space over R
2. R any ring, $M = R^n = \{(x_1, \dots, x_n) : x_n \in R \ \forall n\}$ (with $r(x_1, \dots, x_n) = (rx_1, \dots, rx_n)$)
3. $R = \mathbb{Z}$: ANY abelian group G becomes a $\mathbb{Z}$ module, via $nx = x + \dots + x$ n times (or minus that if n is negative)
   This is the only way to make G a $\mathbb{Z}$ module e.g. $2x = (1+1)x = x + x$
   So $\mathbb{Z}$ modules are equal to Abelian Groups.
4. $R = \mathbb{Z}_6$, $M = \mathbb{Z}_2$ is a $\mathbb{Z}_6$ module, via $r \cdot x = rx \pmod 2$
   (This is well defined as 6 is even)
   More generally, for any ring R, any ideal I is an R-module.
5. $R =$ any ring, $M = R[X]$
6. Let V be a complex vector space, and $\alpha : V \to V$ a linear map.
   Then V is a $\mathbb{C}[X]$ module, via $f \cdot x = f(\alpha)(x)$
   e.g. $(X^2 + 3X + 2) = \alpha^2 x + 3\alpha x + 2x$

Note

In an R-module, $0 \cdot x = 0$ (as $0 \cdot x = (0+0)x = 0x + 0x$, so $0x = 0$ as it is a Group.

Also $(-1)x = -x$ (as $0 \cdot x = (1+(-1))x = x + (-1)x$ so $(-1)x = -1$)

05/03/12

Groups, Rings and Modules (25)

For $x_1, \dots, x_n \in M$, (a module over a ring R), a <u>linear combination</u> is an element of the form $r_1 x_1 + \dots + r_n x_n$ for some $r_1, \dots, r_n \in R$. This is sometimes called an R-linear combination.

We say that the set $x_i : i \in I$ <u>spans</u> M if every $x \in M$ is a (finite) linear combination of the x_i. The set is <u>Linearly Independent</u> if no linear combination is 0 (unless $r_i = 0 \; \forall i$)

A <u>basis</u> is a linearly independent spanning set.

1. e.g. R^n has a basis $l_1, \dots, l_n$ where $l_i = (0, 0, \dots, 0, \underset{i^{th}\text{ place}}{1}, 0, \dots, 0)$
2. $R[X]$ has a basis $1, X, X^2, \dots$

<u>Warnings</u>

1. $R = \mathbb{Z}$, $M = \mathbb{Z}$: $\{2, 3\}$ is spanning, but does not contain a basis
2. $\{2\}$ is linearly independent, but does not extend to a basis.
3. $\mathbb{Z}$ has a basis of size 1 (namely $\{1\}$), but the proper subset $2\mathbb{Z}$ has a basis of the same size (namely $\{2\}$).
4. $\mathbb{Z}$ module $\mathbb{Z}_5$ has no basis, as any single element x is linearly dependent (as $5 \cdot x = 0$).

"For intuition/understanding, think of $R = $ Field and $R = \mathbb{Z}$"

<u>New Modules from Old</u>

<u>Submodules</u>

A <u>submodule</u> of an R-module M is a subset $N \subset M$ that is a module under the induced operation.

i.e. i) N a subgroup of $(M, +)$

ii) $rx \in N$, $\forall r \in R$, $x \in N$

<u>Examples</u>

1. $R = $ Field, M a vector space over R. Then submodules are just subspaces
2. $R = \mathbb{Z}$: Submodules are subgroups.
3. R any ring, $M = R$: Submodules are ideals
4. V a complex vector space, $\alpha: V \to V$ linear, so V is a $\mathbb{C}[X]$ module via $f \cdot x = f(\alpha)(x)$

In this case, submodules are subspaces W that are α-invariant ($\alpha(x) \in W$ $\forall x \in W$, also called 'α acts on W')

For $x_1, \dots, x_n \in M$, the submodule generated by $x_1, \dots, x_n$ is $(x_1, \dots, x_n) = Rx_1 + \dots + Rx_n = \{r_1 x_1 + \dots + r_n x_n : r_1, \dots, r_n \in R\}$
We say M is finitely generated if $M = (x_1, \dots, x_n)$ for some $x_1, \dots, x_n \in M$, the same as saying that $\exists$ a finite spanning set

e.g. $M = R$, an ideal is finitely generated as an R-module
$\Leftrightarrow$ It is finitely generated as an ideal.

Warning A submodule of a finitely generated module need not be finitely generated.
e.g. $R = \mathbb{P}(\mathbb{N})$. Then R is finitely generated ($R = (1)$), but the submodule (ideal) $\{A \subset \mathbb{N} \mid A \text{ finite}\}$ is not finitely generated.

Direct Sums
For R-modules M and N, their direct sum $M \oplus N$ consists of the abelian group $M \times N$, made into an R-module via $r(x,y) = (rx, ry)$
e.g. $R \oplus R = R^2$

Homomorphisms and Quotients
Let M and N be R-modules. A function $\theta : M \to$ is a homomorphism or R-homomorphism if it preserves the module structure.
i.e. θ is a group homomorphism, and $\theta(rx) = r\theta(x)$ $\forall r \in R, x \in M$
If θ is bijective, we say that θ is an isomorphism theorem, and that M and N are isomorphic, written $M \cong N$.

Examples
1. R = Field ; R homomorphisms are linear maps
2. $R = \mathbb{Z}$, ; R homomorphisms are group homomorphisms.
3. If an R module M has a basis, we say that M is free (e.g. $R, R^2, R^3, R[x]$ are all free, $\mathbb{Z}_5$ is not a free $\mathbb{Z}$-module)

05/03/12

Groups, Rings and Modules (20)

If $\exists$ a basis $x_1, \dots, x_n$ of size n, we say that M is free of rank n (e.g. R^n). Note that if M is free of rank n, then $M \cong R^n$, via $\theta : R^n \to M$, $(r_1, \dots, r_n) \mapsto r_1x_1 + \dots + r_nx_n$
(it is not obvious that $R^n \ncong R^m$ when $n \neq m$)

4. Similarly, M finitely generated (i.e. $M = (x_1, \dots, x_n)$) $\Rightarrow$ M is an image of R^n (using the same θ).

The image of θ is $\theta(M) = \{\theta(x) \mid x \in M\}$. This is a submodule of N, as it is certainly a subgroup, and $r\theta(x) = \theta(rx) \in \theta(M)$ $\forall r \in R$, $x \in M$
The kernel of θ is $\ker\theta = \{x \in M \mid \theta(x) = 0\}$. This is a submodule of N, as it is certainly a subgroup, $x \in \ker\theta \Rightarrow \theta(rx) = r\theta(x) = 0$ $\Rightarrow rx \in \ker\theta$. So kernels are submodules. Conversely:

Given an R-module M, and submodule N, the Quotient Module M/N consists of the group M/N, made into an R-module via
$r(x+N) = rx + N$ (well defined, as $x + N = x' + N$
$\Rightarrow x - x' \in N$, $r(x-x') \in N$, $rx + N = rx' + N$)

Note This is an R-module. The projection map $\pi : M \to M/N$, $x \mapsto x + N$ is an R-homomorphism.
This is a group homomorphism, and $\pi(rx) = rx + N = r(x+N) = r\theta(x)$

Proposition: M an R module $N \subset M$.
Then N is a submodule $\Leftrightarrow$ $N = \ker\theta$, for some R-homomorphism $\theta : M \to P$ (some R module P).
Proof
($\Leftarrow$) Kernels are always submodules.
($\Rightarrow$) We have $N = \ker\pi$, where $\pi : M \to M/N$ is the projection map. $\square$.

3

07/03/12

Groups, Rings and Modules (21)

Proposition 2 (Isomorphism Theorem) Let $\Theta : M \to N$ be an R-homomorphism. Then $M/\ker\Theta \cong \Theta(M)$

Proof

We have $f : M/\ker\Theta \to \Theta(M)$, a well defined group isomorphism
$x + \ker\Theta \mapsto \Theta(x)$

Also, $f(r(x + \ker\Theta)) = f(rx + \ker\Theta) = \Theta(rx) = r\Theta(x) = rf(x + \ker\Theta)$

We know that M finitely-generated (say by $x_1, \dots, x_n$)
$\Rightarrow$ M is an image of R^n by $\Theta : R^n \to M$, $(r_1, \dots, r_n) \mapsto r_1x_1 + \dots + r_nx_n$
So finitely generated R-modules are quotients of R^n ($n = 1, 2, 3, \dots$)

~~A module~~

A module is cyclic if it is generated by 1 element.
e.g. If R is a field: The cyclic R-modules are $\{0\}$ and R.
$R = \mathbb{Z}$: The cyclic $\mathbb{Z}$ modules are the cyclic groups ($\mathbb{Z}$ and $\mathbb{Z}_n$, any n)

Note

M cyclic $\Leftrightarrow$ M an image of $R^1 \Leftrightarrow M \cong R/I$, for some I

The Structure Theorem

We know a structure theorem for finitely generated modules over a field F, They are $F^n = F \oplus \dots \oplus F$ ($n = 0, 1, 2$). What about over a general ring?

Aim

For R a Euclidean Domain, every finitely-generated R-module is a direct sum of (finitely many) cyclic modules ← The best we could possibly hope for

e.g. $R = \mathbb{Z}$:
Every finitely-generated Abelian Group is of the form $\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z} \oplus \dots$
(so every finite Abelian Group is of the form $\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$)

Remark Let R be $\mathbb{Z}[x]$ and consider the R-module $M = (2, x) \subset R$
Then M is not a direct sum of cyclic modules.
Indeed, M itself is not cyclic (as $(2, x)$ is not principal).
And if M was a direct sum of more than one R-module, choose non-zero a, b in distinct summands. e.g. $M = M_1 \oplus M_2 \oplus \dots$ with $a \in M_1$, $b \in M_2$

Then $a \cdot b = b \cdot a$, so the two summands react $\oplus$ ← a direct sum $\square$

<u>Task</u> Understand finitely generated R-modules i.e. R^n/N, where N is a submodule of R^n.

<u>Key Idea</u>

R^n/N is easy to describe if N "lines up nicely" with respect to the axes of R^n.

<u>Examples</u> $(R = \mathbb{Z})$ $\quad e_1 = (1,0)$

1. What is $\mathbb{Z}^2/\langle 3e_1, 7e_2\rangle$? $\quad e_2 = (0,1)$

   $\langle \cdot \rangle$ means "sub-module generated by"

   It is $\mathbb{Z}_3 \oplus \mathbb{Z}_7$

   (This is obvious, but formally $\theta : \mathbb{Z}^2 \to \mathbb{Z}_3 \oplus \mathbb{Z}_7$, $(x,y) \mapsto (x,y)$, $\ker\theta$ as required

2. What is $\mathbb{Z}^2/\langle 3e_1\rangle$?

   It is $\mathbb{Z}_3 \oplus \mathbb{Z}$.

3. What is $\mathbb{Z}^2/\langle (3,6)\rangle$? ← Not obvious, because the generators of the subgroup do not 'line up' with respect to our basis e_1, e_2 of $\mathbb{Z}^2$.

We have a basis $f_1 = (1,2)$, $f_2 = (0,1)$

(These are certainly linearly independent, and span because $e_1 = f_1 - 2f_2$, $e_2 = f_2$), and now our quotient is $\mathbb{Z}^2/\langle 3f_1\rangle$, which is $\mathbb{Z}_3 \oplus \mathbb{Z}$.

Let A be an $m \times n$ matrix over a ring R. (→ m rows, n columns)

The <u>elementary row operations</u> on A are:

1. Swap two rows
2. Multiply a row by a <u>unit</u>
3. Subtract a multiple of a row from another row.

This works similarly for column operations

<u>Theorem 3</u> Let A be a matrix over a Euclidean Domain. Then $\exists$ a finite sequence of elementary row and column operations that puts A into $\left(\begin{array}{ccc|c} d_1 & & 0 & \\ & d_2 & & 0 \\ 0 & & \ddots\, d_k & \end{array}\right)$ where $d_1 | d_2 | \dots | d_k$

09/03/12

Groups, Rings and Modules (22)

Proof

If $A=0$ we are done. If $A \neq 0$ WLOG $a_{11} \neq 0$
(otherwise, use rows and column swaps)
Using elementary operations, we produce

either $\begin{pmatrix} a_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & B \\ 0 & \end{pmatrix}$ with a_{11} dividing each entry of B (so we are done by induction

or $\begin{pmatrix} a_{11}' & \\ & \\ & \end{pmatrix}$ with $\varphi(a_{11}') < \varphi(a_{11})$, (then repeat, and we are done as we cannot decrease φ infinitely often)

Write $b = a_{11}$

Suppose some entry of the top row is not a multiple of b, say a, in column j.

$\begin{pmatrix} b & & a & \\ & & & \\ & & & \end{pmatrix}$

Write $a = qb + r$, $\varphi(r) < \varphi(b)$

Now replace column j with column j + q column 1
and then swap columns 1 and j.

Hence, we may assume that all entries of row 1, column 1 are multiples of b. So, by subtracting multiples of row 1 or column 1, we can make all entries in row 1 and column 1 (except a_{11}) zero.

Suppose some entry b_{ij} of this matrix is not a multiple of b. Add row i to row 1: We now have an entry of row 1, not a multiple of b, so we are done as before.

$\begin{pmatrix} b & 0 & 0 \cdots & 0 \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$

Remarks

1. Sometimes, we say $n \times n$ matrices A, B are equivalent if one can be obtained from the other by elementary operations. So Theorem 3 says that any matrix A is equivalent to one of the form $\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{pmatrix}$
2. The d_i are invariant factors for A, and the matrix is called a Smith-Normal Form.
3. In the language of linear maps: Let $\theta : R^n \to R^m$ be an R homomorphism and $\underline{e}_1, \dots, \underline{e}_n$ basis vectors for R^n, $\underline{f}_1, \dots, \underline{f}_m$ basis vectors for R^m. The matrix of θ with respect to $\underline{e}_1, \dots, \underline{e}_n$ and $\underline{f}_1, \dots, \underline{f}_m$ is the $m \times n$ matrix, $A = (a_{ij})$ given by the following:

$$\begin{array}{c|c} & e_1 \;\cdots\cdots\; e_n \\ \hline \begin{array}{c} f_1 \\ \vdots \\ f_m \end{array} & \left(\begin{array}{c} \uparrow \\ \theta(e_1) \text{ in terms of the } f_i \\ \downarrow \end{array} \quad\quad\quad \right) \end{array} \qquad \theta(\underline{e}_j) = \sum_i a_{ij} \underline{f}_i$$

Then row operations correspond to changes in the basis $\underline{f}_1, \dots, \underline{f}_m$ and column operations to changes in $\underline{e}_1, \dots, \underline{e}_n$.
(e.g. "Swap rows 1 and 2" replaces $\underline{f}_1, \underline{f}_2, \dots, \underline{f}_m$ with $\underline{f}_2, \underline{f}_1, \dots, \underline{f}_m$)
So Theorem 3 is saying that $\exists$ bases with respect to which θ has a diagonal matrix.

4. <u>Hideous Remark</u> Row ops correspond to pre-multiplying A by an invertible matrix, e.g. "Swap rows 1 and 2" is pre-multiplying A by $\underset{m \times m}{\begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & 0 \\ & 1 & \\ 0 & & \ddots \; 1 \end{pmatrix}}$. Similarly, column operations correspond to post multiplication.
So Theorem 3 tells us that $\exists$ an invertible $m \times m$ P, $n \times n$ Q with $PAQ = D$, diagonal.

<u>Corollary 4</u> Let R be a Euclidean Domain. Then $R^m \not\cong R^n$ for $m \neq n$.
Note: this is <u>not</u> obvious as we do <u>not</u> have an Exchange Lemma.
<u>Proof</u> Say $n > m$. Suppose $\theta : R^n \to R^m$ is an isomorphism. Then, by our linear map form of Theorem 3, $\exists$ bases $\underline{e}_1, \dots, \underline{e}_n$ of R^n, and $\underline{f}_1, \dots, \underline{f}_m$ of R^m, with respect to which θ has matrix

$$m \left(\begin{array}{ccccc} d_1 & & & & \\ & \ddots & & & 0 \\ & & d_k & & \\ 0 & & & 0 & \\ & & & & \ddots \; 0 \end{array} \right)$$

But then, $\theta(\underline{e}_n) = 0$ $\#$

$\square$

<u>Remarks</u>
1. Hence, all bases of R^n have size n.
2. In fact $R^n \not\cong R^m$ for any ring R, but this is harder to prove.

09/03/12 Groups, Rings and Modules (22)

Uniqueness in Smith-Normal Form

For an $m \times n$ matrix A, over a Euclidean Domain R, a $t \times t$ minor of A is the determinant of any $t \times t$ sub-matrix of A.

e.g. over $\mathbb{Z}$ $\begin{pmatrix} 2 & 1 & 4 \\ 7 & 3 & 6 \\ 8 & 7 & 1 \end{pmatrix}$ has a 2×2 minor $\det\begin{pmatrix} 1 & 4 \\ 7 & 1 \end{pmatrix} = -27$

Note: For 'det' we have a choice.

Either define $\det X = \sum_{\sigma \in S_t} \epsilon(\sigma) x_{1\sigma(1)} \dots x_{t\sigma(t)}$

or entries are in the field of fractions of R, so we already have det

Note that row and column operations do not change the HCF of the $t \times t$ minors (for any fixed t).

Indeed:

1. Multiplying a row by a unit does not change any $t \times t$ minor (up to multiplying some by that unit)
2. Swapping two rows permutes the $t \times t$ minors (up to a factor -1)
3. Adding $\lambda \times$ row j to row i : a minor involving both rows i and j or neither is unchanged.

Finally, consider $t\times t$ submatrices A, B, identical except that A has row i (and not row j) while B has row j (and not row i).

Let $a = \det A$, $b = \det B$

Then the new b has $\det B = b$, and the new A has $\det = a + \lambda b$

But $HCF(a + \lambda b, b) = HCF(a, b)$

3

12/03/12

Groups, Rings and Modules (23)

<u>Theorem 5</u> Let A be an $m \times n$ matrix over R, a Euclidean Domain with Smith-Normal form $B = \begin{pmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_k & \\ 0 & & & 0_0 \end{pmatrix}$ where non-zero $d_1 | d_2 | \dots | d_k$ (and set $d_{k+1} = d_{k+2} = \dots = 0$)

Then $\forall t$: $d_1 \dots d_t$ = HCF of $t \times t$ minors of A (up to associate)

In particular, the Smith Normal form is unique (up to multiplying a d_i by a unit).

<u>Proof</u> Elementary operations do not change the HCF of $t \times t$ minors, so the HCF of the $t \times t$ minors of A = HCF of $t \times t$ minors of B

$= d_1 \dots d_t$ (where we used $d_1 | d_2 | \dots | d_k$) $\square$

<u>Example</u> ~~(Slow way)~~

Smith-Normal Form of $\begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix}$ over $\mathbb{Z}$

Good if we have non zero entries → <u>Slow way</u>: $\begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} \to \begin{pmatrix} -1 & 3 \\ -4 & 8 \end{pmatrix}$ (column 1 $\mapsto$ column 1 − column 2)

$\to \begin{pmatrix} 1 & -3 \\ -4 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ -4 & -4 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -4 \end{pmatrix}$

row 1 $\mapsto$ − row 1   column 2 $\mapsto$ column 2 + 3 column 1   row 2 $\mapsto$ row 2 + 4 row 1

Good if there are lots of zeros → <u>Fast way</u>: HCF of 1×1 minors = HCF of entries = 1

For the 2×2 minors, $\det \begin{pmatrix} 2 & 3 \\ 4 & 8 \end{pmatrix} = 4$, so $d_1 = 1$, $d_1 d_2 = 4$, $\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$

One final ingredient:

<u>Lemma 6</u> Let R be a Euclidean Domain. Then every sub-module of R^n is finitely generated.

<u>Proof</u> (by induction on n)

True for $n = 1$, as submodules of R are ideals of R, and all principal.

Given N, a sub-module of R^n, for some $n > 1$:

Let $I = \{ r \in R : (r, r_2, \dots, r_n) \in N$ for some $r_2, \dots, r_n \in R \}$

Then I is an ideal of R, so $I = (a)$ for some $a \in R$.

Choose $x = (x_1, \dots, x_n) \in N$ with $x_1 = a$.

Let $N' = \{ (r_2, \dots, r_n) \in R^{n-1} : (0, r_2, r_3, \dots, r_n) \in N \}$

Then N' is a submodule of R^{n-1}, so by induction, we have that $N' = \langle y^{(1)} \dots y^{(k)} \rangle$ for some $y^{(1)} \dots y^{(k)} \in R^{n-1}$

Thus x, $(0, y^{(1)}), \dots, (0, y^{(k)})$ generate N. Indeed, if $y \in N$, then $\exists\, r \in R$ with $y - rx$ of the form $(0, r_2, \dots, r_n)$ which is a linear combination of the ~~forms~~ $(0, y^{(i)})$ $\square$

Theorem 7 Let N be a submodule of R^n (with R a Euclidean domain)
Then $\exists$ a basis $\underline{e_1}, \ldots, \underline{e_n}$ of R^n and non-zero $d_1, \ldots, d_k \in R$ (for some k)
such that $N = \langle d_1 \underline{e_1}, \ldots, d_k \underline{e_k} \rangle$ $\Leftarrow$ i.e. "N lines up nicely"

Proof

$\Leftarrow$ not assuming they are a basis for N

Let $\underline{e_1}, \ldots, \underline{e_n}$ be a basis of R^n, and let $g_1, \ldots, g_m$ generate N
Let $A = \{a_{ij}\}$ be matrix of the g_j with respect to the $\underline{e_i}$, $g_j = \sum_i a_{ij} \underline{e_i}$

$$\begin{array}{c} \\ \underline{e_1} \\ \vdots \\ \underline{e_n} \end{array} \begin{array}{c} g_1 \ \cdots \ g_m \\ \left(\begin{array}{c} \uparrow \\ g_j \text{ in terms of the } \underline{e_i} \\ \downarrow \end{array} \right) \end{array}$$

We can transform A to $\begin{pmatrix} d_1 & & & \\ & \ddots & & 0 \\ & & d_k & \\ 0 & & & 0 \end{pmatrix}$ by elementary operations.

Now, row operations correspond to changing the basis of R^n, and column operations to changing the generators of N.
Hence $\exists$ a basis $\underline{e_1}', \ldots, \underline{e_n}'$ for R^n such that N has generators $d_1\underline{e_1}', \ldots, d_k\underline{e_k}'$ $\square$

Corollary 8 Every submodule of R^n (R a Euclidean Domain) is free (and of rank $\leq n$.)

Proof

Certainly $d_1 \underline{e_1}', \ldots, d_k \underline{e_k}'$ are linearly independent (any dependence would be a dependence among $\underline{e_1}', \ldots, \underline{e_k}'$) $\square$

Remarks

1. In fact, a submodule of any free R-module (R a Euclidean domain) is free (harder to prove)
2. Let $R = \mathbb{Z}[x]$. Then the R-module $\mathbb{Z}[x]$ is free (it's R^1) but the sub-module $(2, x)$ is not free, and not even a direct sum of any non-zero submodules.

GMV

14/03/12

Groups, Rings and Modules (24)

Corollary 9 (Structure Theorem for (finitely generated) modules over a Euclidean domain)
Let M be a finitely generated module over a Euclidean Domain R. Then M is a (finite) direct sum of cyclic modules.

Proof
We know that $M \cong R^n/N$ for some n, and N a sub-module of R^n, and we know that $\exists$ a basis $e_1, \dots, e_n$ of R^n with respect to which $N = \langle d_1 e_1, \dots, d_k e_k \rangle$ for some k, and $d_1, \dots, d_k \in R$.
But then, $R^n/N \cong R/(d_1) \oplus \dots \oplus R/(d_k) \oplus \underbrace{R \oplus \dots \oplus R}_{n-r \text{ times}}$ □

Corollary 10
Every finitely generated Abelian group is a (finite) direct sum of cyclic groups.

Proof
Put $R = \mathbb{Z}$ □.

For G a finite abelian group, we know that $G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}$ using $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ for m, n coprime, we can further 'break up' G, obtaining $G \cong \mathbb{Z}_{p_1^{a_1}} \oplus \mathbb{Z}_{p_2^{a_2}} \oplus \dots \oplus \mathbb{Z}_{p_n^{a_n}}$, some $p_1, \dots, p_n$ primes, $a_1, \dots, a_n \geq 0$.
[In general, a cyclic R-module R/I is called primary if $I = (p^a)$, some prime p in R, or $I = \{0\}$] $\Leftarrow$ R / (power of a prime ideal)

In fact, the $p_i^{a_i}$ are unique (up to reordering). Indeed for p prime, $|G|/|pG| = p \wedge (\# \, p_i^{a_i} \text{ with } a_i \geq 1)$

and $|G|/|p^2G| = p \wedge (\# \, p_i^{a_i} \text{ with } a_i \geq 1 + \# \text{ with } a_i \geq 2)$ etc

Generalising "$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$":
Proposition 11 (Chinese Remainder Theorem)
Let R be a PID, and let $r, s \in R$ be coprime (i.e. $HCF(r,s) = 1$)
Then $R/(rs) \cong R/(r) \oplus R/(s)$ (isomorphic as R-modules)

Proof
Define $\theta : R \to R/(r) \oplus R/(s)$, $x \mapsto (x + (r), x + (s))$
Then θ is an R-homomorphism with $\ker\theta$, $\ker\theta = (r) \cap (s) = (rs)$ (as r, s are coprime and R is a UFD).
Also, we have $1 = xr + ys$, some $x, y \in R$, (as r, s are coprime, and R a PID)
So $\theta(xr) = (0,1)$ and $\theta(ys) = (1,0)$ and so θ is surjective.
Thus $R/(rs) \cong R/(r) + R/(s)$ □
Note: the same proof shows that $R/(rs) \cong R/(r) \oplus R/(s)$ as rings.

Corollary 12 (Primary Decomposition Theorem)
Let M be a finitely generated module over a Euclidean Domain R. Then M is a (finite) direct sum of primary modules ($R/(p^a)$ or R)

Proof By the Structure Theorem, followed by the Chinese Remainder Theorem. □

Jordan-Normal Form

V a finite dimensional complex vector space, $\alpha : V \to V$ a linear map. V is a $\mathbb{C}[X]$ module via $f \cdot x = f(\alpha)(x)$ for $x \in V$, $f \in \mathbb{C}[X]$

We know that V is a direct sum of primary sub-modules. What does a primary submodule W look like? W has one generator, say x, and $W \cong \mathbb{C}[X]/(x-\lambda)^t$ for some $\lambda \in \mathbb{C}$, some t.

(Because the only irreducibles in $\mathbb{C}[X]$ are degree 1, by the Fundamental Theorem of Algebra)

(Also note, $W \not\cong \mathbb{C}[X]$, otherwise $x, \alpha x, \alpha^2 x, \ldots$ are linearly independent ※)

Thus, elements of W are all of the form $f(\alpha)(x)$, where $\deg f \leq t$, and these are all distinct. So $x, (\alpha-\lambda)x, (\alpha-\lambda)^2 x, (\alpha-\lambda)^{t-1}x$ are linearly independent and span W, so are a basis for W.

The matrix of $\alpha - \lambda$ with respect to this basis is $\begin{pmatrix} 0 & 0 & & 0 & 0 \\ 1 & 0 & \ddots & & 0 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & 0 & \vdots \\ 0 & 0 & & 1 & 0 \end{pmatrix}$

So α has a matrix $\begin{pmatrix} \lambda & & 0 \\ 1 & \ddots & \\ 0 & 1 & \lambda \end{pmatrix}$ with respect to this basis (a λ block of size d or dimension d)

Hence:

Corollary 13

A linear map on a finite dimensional complex vector space V has matrix (with respect to some basis) that is a diagonal sum of λ blocks (for various λ) $\square$

Remarks

1. Given this 'Jordan-Normal Form', we can read off many properties of α, for example, for an eigenvalue λ, the algebraic multiplicity (as a root of the characteristic polynomial) = sum of sizes of λ blocks

   geometric multiplicity (dimension of the eigenspace) = # λ blocks

   the minimum polynomial multiplicity (as a root of the minimum polynomial) = size of the biggest λ block.

2. The Jordan Normal Form is unique (up to reordering of blocks). Indeed,
   $\dim(\ker(\alpha-\lambda))$ = # λ blocks
   $\dim(\ker(\alpha-\lambda)^2)$ = # λ blocks + # λ blocks of size ≥ 2 etc
   (this is really the same idea as for our finite abelian groups)