7202 Algebra 4: Groups and Rings Notes

Based on the 2017 spring lectures by Prof F E A Johnson

MATH 7202

10-01-17

Hw due on Fridays for now.

Room 705

Don't go on Thursday!

A group consists of a triple $G = (G, \square, e)$

i). G is a set

ii). $e \in G$

iii). $\square : G \times G \longmapsto G$ mapping

$\square(g, h) = g \square h$

such that

a). $\square$ is associative

$(g \square h) \square k = g \square (h \square k)$

b). $\forall g \in G \quad g \square e = e \square g = g$, e is an identity

c). $\forall g \in G \quad \exists g^* \in G$ s.t. $g \square g^* = e = g^* \square g$, g^* is an inverse

Two standard conventions

- Multiplicative notation $\square = \cdot$, $e = 1$, $g^* = g^{-1}$

$g \cdot 1 = 1 \cdot g = g \quad \forall g \in G$, $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

$g \cdot g^{-1} = 1 = g^{-1} \cdot g$

$(G, e, \square)$ is called abelian (NH Abel 1799-1826) when

$\forall g, h \in G, \; g \square h = h \square g$

- Additive notation $\square = +$, $e = 0$, $g^* = -g$

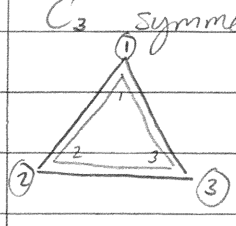
$\forall g \in G \quad g + 0 = 0 + g = g$, $(g+h)+k = g+(h+k)$

$\forall g \; \exists -g \in G$ s.t. $g + (-g) = 0 = (-g) + g$

(E. Galois 1811-1832)

Example

C_3 symmetries of an 1-sided equilateral triangle



Id: ${}_2\triangle^1{}_3$

rotate anticlockwise by $\frac{2\pi}{3}$ (x) : ${}_1\triangle^3{}_2$

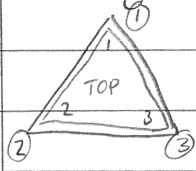
x^2 : ${}_3\triangle^2{}_1$

$x^3 = \text{Id}$

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

Example

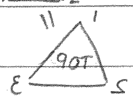
D_6 : symmetries of a 2-sided equilateral triangle



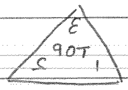
id : 

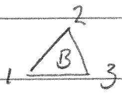
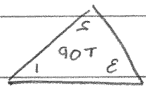
x :  $x^3 = 1$

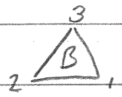
flip about vertex 1 y :  $y^2 = 1$

$\parallel$ 

Compose functionally, xy = first y then x.

yx :  = 

xy :  =  $yx \neq xy$

x^2y :  $= yx$

So if we analyze symmetries of a 2-sided $\triangle$,
x = rotation through $2\pi/3$ (no flip) ↺
y = flip about a pre-specified vertex.
$x^3 = 1, \quad y^2 = 1, \quad yx = x^2y$

D_6

$\cdot$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

$$yx^2 = (yx)x = (x^2y)(x) = x^2(yx) = x^2(x^2y) = xy$$
$$yxy = x^2yy = x^2$$
$$yx^2y = y^2x = x$$
$$x(yx) = x(x^2y) = y$$
$$xyx^2 = xxy = x^2y.$$
$$xyxy = xx^2yy = x^3y^2 = 1$$

$$x^2yx^2y = x^2xy^2 = x^3y^2 = 1$$

$$xy\,x^2y = x(xy)y = x^2y^2 = x^2$$
$$x^2yx = x^4y = xy$$
$$x^2yx^2 = x^2xy = x^3y = y$$
$$x^2y^2 = x^2$$
$$x^2yxy = yx^2y = y^2x = x$$

MATH 7202

10-01-17

$C_3 = \langle x \mid x^3 = 1 \rangle = \{1, x, x^2\}$ ← Cyclic group of order 3

$D_6 = \langle x, y \mid x^3 = 1, y^2 = 1, yx = x^2 y \rangle = \{1, x, x^2, y, xy, x^2 y\}$

↖ Dihedral group of order 6

Generalisations

$C_n = \langle x \mid x^n = 1 \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$

Cyclic group of order n

(Symmetries of a 1-sided regular n-gon) with x being a rotation through $\frac{2\pi}{n}$ anticlockwise.

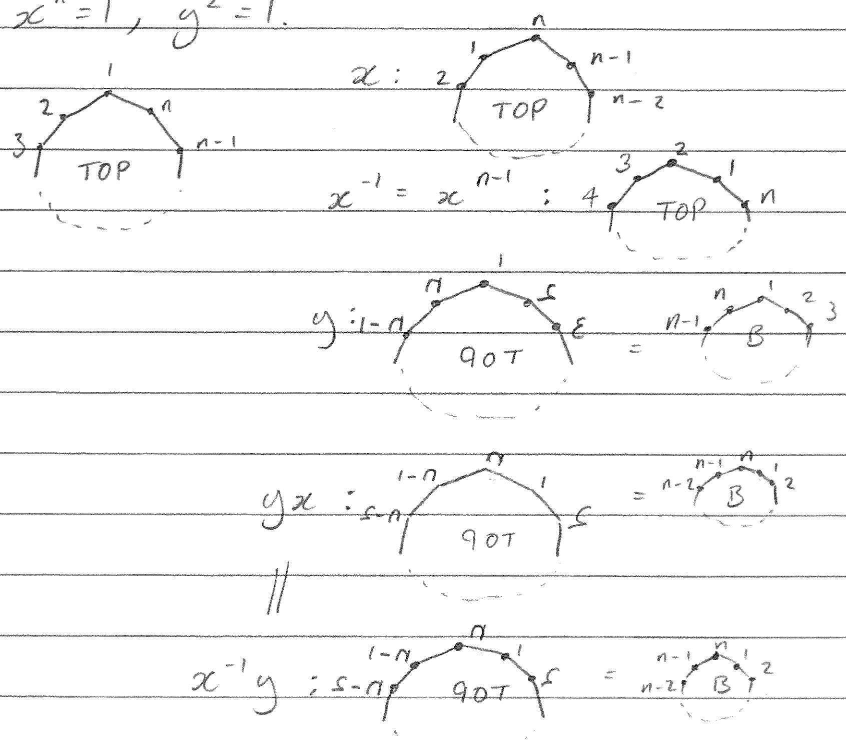
Special case: $C_2 = \{1, x \mid x^2 = 1\}$

	1	x
1	1	x
x	x	1

$\cong$

	1	-1
1	1	-1
-1	-1	1

D_6 generalises to D_{2n} = symmetries of a 2-sided regular n-gon. x rotates through $\frac{2\pi}{n}$ anticlockwise, and y flips about vertex n, a pre-specified position, $x^n = 1$, $y^2 = 1$.



So $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yx = x^{n-1} y \rangle$ (for multiplication)

$C_n = \langle x \mid x^n = 1 \rangle \quad n = 1, 2, 3, \ldots$

$D_{2n} = \langle x, y \mid x^n = 1,\ y^2 = 1,\ yx = x^{n-1}y \rangle$

nonabelian for $n \geq 3$

Special case: $D_4 = \langle x, y \mid x^2 = 1,\ y^2 = 1,\ yx = xy \rangle \quad (n = 2)$

$[= C_2 \times C_2]$

D_4	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

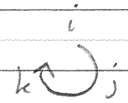
$xyxy = xxyy = 1 \cdot 1 = 1$

Exercise: Realise D_4 as a 2-sided, genuine rectangle (not square).

$Q(8)$: quaternion group of order 8 (First observed by Hamilton)

$Q(8) = \{1, -1, i, -i, j, -j, k, -k\}$

$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1, \quad ij = k = -ji$



$$\begin{cases} ij = k = -ji \\ jk = i = -kj \\ ki = j = -ik \end{cases}$$

$Q(8)$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(non abelian)

MATH 7202

10-01-17

$Q(8)$ is nonabelian of order 8
D_8 " " " " 8
Are they the same or different?

D_8	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1							
x		x^2						
x^2			1					
x^3				x^2				
y					1			
xy						1		
x^2y							1	
x^3y								1

They are different!

Def^n
Let G be a finite group and $g \in G$.
Define $\mathrm{ord}(g) = \min(r : g^r = 1)$

In D_8 every non-trivial element has order $= 2$ except for x, x^3.
$\mathrm{ord}(x) = 4$, $\mathrm{ord}(x^3) = 4$

Prop
$\mathrm{ord}(g) = 2$ $(g \neq 1)$ iff $g^2 = 1 \Leftrightarrow g = g^{-1}$

Prop
$\mathrm{ord}(1) = 1$, $1^{-1} = 1$.

In $Q(8)$ the only non trivial element of order 2 is -1.
All other non-trivial elements have order 4

Def^n

Let $G = (G, 1, \cdot)$, $H = (H, 1, \square)$ both be groups.
By a homomorphism $\varphi : G \mapsto H$ we mean a mapping with property that $\varphi(x \cdot y) = \varphi(x) \square \varphi(y)$ $\forall x, y \in G$.

MATH 7202

17-01-17

Suppose $G = (G, \square, e)$, $H = (H, *, E)$ are groups.
By a homomorphism
$$\varphi : G \longrightarrow H$$
we mean a mapping with the property
$$\varphi(g_1 \square g_2) = \varphi(g_1) * \varphi(g_2)$$
ie. it preserves group operation.

Prop
If φ is a homomorphism
$$\varphi(e) = E.$$
(φ takes identity to identity)

Proof
$$e \square e = e$$
So $\varphi(e) * \varphi(e) = \varphi(e)$
Multiply on right by $\varphi(e)^{-1}$
$$\Rightarrow \quad \varphi(e) * \varphi(e) * \varphi(e)^{-1} = \varphi(e) * \varphi(e)^{-1}$$
$$= E$$
$$\Rightarrow \quad \varphi(e) * E = E$$
$$\Rightarrow \quad \varphi(e) = E \qquad \square$$

First historical example is
$G = (\mathbb{R}, +, 0)$ (additive reals)
$H = (\mathbb{R}_{>0}, \cdot, 1)$ (multiplicative group of positive reals)
$$\exp : \mathbb{R} \mapsto \mathbb{R}_{>0}, \quad \exp(x) = \sum_{r=0}^{\infty} \frac{x^r}{r!}$$

$$\left.\begin{array}{l} \exp(x+y) = \exp(x)\exp(y) \\ \exp(0) = 1 \end{array}\right\} \text{homomorphism}$$

Second historical example
$$\log : \mathbb{R}_{>0} \mapsto \mathbb{R}$$
$\log(xy) = \log(x) + \log(y)$
$\log(1) = 0$ (Napier)

In purely multiplicative notation

$$\varphi : (G, \cdot, 1_G) \mapsto (H, \cdot, 1_H)$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

So by above $\varphi(1_G) = 1_H$

Prop

If $\varphi : G \mapsto H$ is a homomorphism, then $\forall g \in G$

$$\varphi(g^{-1}) = \varphi(g)^{-1}$$

Proof

$$g \cdot g^{-1} = 1_G$$

Apply φ:

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(1_G) = 1_H$$

Also:

$$g^{-1} \cdot g = 1_G$$

$$\Rightarrow \varphi(g^{-1}) \cdot \varphi(g) = \varphi(1_G) = 1_H.$$

So $\varphi(g^{-1})$ is a two-sided inverse for $\varphi(g)$

i.e. $\varphi(g^{-1}) = \varphi(g)^{-1}$. $\square$.

Def.

Let G, H be groups and $\varphi : G \mapsto H$ be a homomorphism.
We say that φ is an isomorphism when φ is bijective.

e.g. $\exp : \mathbb{R} \mapsto \mathbb{R}_{>0}$ is an isomorphism.
exp is bijective so it has an inverse

$$(\exp)^{-1} = \log : \mathbb{R}_{>0} \mapsto \mathbb{R} \quad , \quad \log(x) = \int_1^x \frac{dt}{t},$$

and log is also a homomorphism.

MATH 7202

17-01-17

Prop

If $\varphi : G \mapsto H$ is a bijective homomorphism then $\varphi^{-1} : H \mapsto G$ is also a homomorphism.

Proof

$\varphi(\varphi^{-1}(h_1 h_2)) = h_1 h_2$

$\varphi(\varphi^{-1}(h_1)\varphi^{-1}(h_2)) = \varphi(\varphi^{-1}(h_1))\,\varphi(\varphi^{-1}(h_2))$ (φ homo.)

$= h_1 h_2$

So $\varphi[\varphi^{-1}(h_1 h_2)] = \varphi[\varphi^{-1}(h_1)\varphi^{-1}(h_2)]$

But φ is injective so

$\varphi^{-1}(h_1 h_2) = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$ $\square$.

i.e. the inverse of an isomorphism is an isomorphism.

Problem

Let n be a positive integer.
Describe, up to isomorphism, all groups of order n.

By "up to isomorphism" we mean that if two groups G, H look different, but are isomorphic then we count them as "the same".

e.g. I can describe the cyclic group C_2 in two different ways:

$\cdot$	1	x
1	1	x
x	x	1

$+$	0	1
0	0	1
1	1	0

Consider $Q(8) = \{\pm 1, \pm i, \pm j, \pm k\}$, $D_8 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$

We'll show that $Q(8) \not\cong D_8$

In this case there is a really easy way of doing it.

We say an element $g \in G$ is self-inverse when

$g^{-1} = g \Leftrightarrow g^2 = 1$ (rare occurence in general).

If $\varphi: G \mapsto H$ is an isomorphism and $g \in G$ is self-inverse, then
$\varphi(g) \in H$ is also self-inverse:
$g \cdot g = 1_G \Rightarrow \varphi(g) \cdot \varphi(g) = 1_H$.

Prop
If $\varphi: G \mapsto H$ is an isomorphism, then the number of self inverse elements in G = the number of self inverse elements in H.

Corollary
$Q(8) \ncong D_8$

Proof
$Q(8)$ has two self-inverse elements; $1, -1$.
However, D_8 has six self-inverse elements; $1, x^2, y, xy, x^2y, x^3y$.
$\square$

Order of an element
Let G be a group, $g \in G$.
We say that g has finite order when $\exists n \geq 1$ s.t. $g^n = 1$.
(need $n \geq 1$ since, by convention, $g^0 = 1$.)
If g has finite order, then $\mathrm{ord}(g) = \min\{n \geq 1 : g^n = 1\}$.
The only element of order 1 is the identity

Prop
Let G be a finite group, then every $g \in G$ has finite order.

Proof
Suppose $g \neq 1$.
Consider the mapping $\mathbb{Z}_+ \mapsto G$, $n \mapsto g^n$.
$\mathbb{Z}_+$ is infinite, G finite, so the mapping is therefore

MATH 7202

17-01-17

not injective.
So $\exists\ k, m\ ;\ 1 \leq k < m$
such that $g^k = g^m$.
Multiply across by $(g^{-1})^k = g^{-k}$
$$1 = g^m g^{-k} = g^{m-k}$$
Put $n = m-k \Rightarrow g^n = 1$ □.

Note that in $G = \mathbb{Z}$, every non zero element has ∞ groups.

Example
$C_n = \{1, x, \ldots, x^{n-1}\}$ generated by x, $\operatorname{ord}(x) = n$.
Suppose N is some integer $\geq n$ s.t. $x^N = 1$.
Then n divides N.
Otherwise $N = nq + r$, $0 \leq r < n$.
Suppose $r \neq 0$, then
$$x^N = x^{nq+r} = (x^n)^q x^r$$
$\Rightarrow 1 = 1 \cdot x^r \Rightarrow x^r = 1$
but $1 \leq r < n$ which contradicts the fact that $\operatorname{ord}(x) = n$. □

$C_n = \{1, x, x^2, \ldots, x^{n-1}\}$, $x^n = 1$, $\operatorname{ord}(x) = n$
Take $x^r \in C_n$.
Compute $\operatorname{ord}(x^r)$

Proof
Put $k = \operatorname{ord}(x^r)$
$$= \min\{s \geq 1 : (x^r)^s = 1\} = \min\{s \geq 1 : x^{rs} = 1\}$$
By last lecture, if $x^{rs} = 1$ then rs is a multiple of n.
rs is obviously a multiple of r.
rs is a common multiple of r, s.

s is minimised by $k = \text{ord}(x^r)$
precisely when

$$rk = LCM(r, n)$$

$$rk = \frac{rn}{HCF(r,n)}$$

$$\text{so } k = \frac{n}{HCF(n,r)} \qquad \square$$

Corollary

If $g \in C_n$ then $\text{ord}(g)$ divides n.

This statement generalises.

Prop ← "Cauchy's Theorem"

If G is a finite group and $g \in G$ then $\text{ord}(g)$ divides $|G|$.

"Cauchy's Thm" follows from Lagrange's Thm.

Def.

Let G be a group and let $H \subset G$.
We say that H is a subgroup of G when
(i) $1_G \in H$
(ii) if $x, y \in H$ then $xy \in H$
(iii) if $x \in H$ then $x^{-1} \in H$
(if G is finite then (iii) is redundant).

Example

$G = D_8 = \{1, x, x^2, y, xy, x^2y\}$, $x^3 = 1$, $y^2 = 1$, $yx = x^2y$.
Subgroups of D_8 include $\{1, x, x^2\}$, $\{1, y\}$, $\{1, xy\}$, $\{1, x^2y\}$.
Non-examples of subgroups = $\{1, x\}$, $\{1, y, xy\}$. ← not subgroups!

MATH 7202

17-01-17

Any group G has two obvious subgroups:
(i) G , (ii) $\{1\}$.

Theorem (Lagrange c1780)
If G is a finite group, and $H \subset G$ is a subgroup, then $|H|$ divides $|G|$ exactly.

Cosets
Let G be a group, $H \subset G$ a subgroup.
If $g \in G$, define

$gH = \{gh : h \in H\}$ (left coset of H by G).
$Hg = \{hg : h \in H\}$ (Right coset of H by G).

(We usually work with gH)

Example
$G = D_6 = \{1, x, x^2, y, xy, x^2y\}$
$H = \{1, y\}$
Take $g \in D_6$ in turn and compute gH

$1 \cdot H = \{1, y\}$ $=$ $yH = \{y, y^2\} = \{y, 1\}$
$xH = \{x, xy\}$ $=$ $xyH = \{xy, xy^2\} = \{xy, x\}$
$x^2H = \{x^2, x^2y\}$ $=$ $x^2yH = \{x^2y, x^2y^2 = \{x^2y, x^2\}$

Definition
G/H = set of left cosets of H
$= \{gH : g \in G\}$

remember brakets!

In this case $G/H = \{\{1, y\}, \{x, xy\}, \{x^2, x^2y\}\}$

$|G/H| = 3 = 6/2 = |G|/|H|$

The snag with cosets is that they can be described in more than one way.

e.g. $xH = xyH$ (as above) but $x \neq xy$.

Rule of equality for cosets

Let G be a group and H a subgroup

Then $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H$.

Proof

First consider, when is it true that $gH = H$?

$gH = H \iff g \in H$.

If $gH = H$, $g = g \cdot 1 \in gH = H$

$gH = H \Rightarrow g \in H$.

If $g \in H$ and $h \in H$ then $gh \in H$, H is a subgroup

so $gH \subset H$.

Conversely if $h_1 \in H$,

then $g \in H$ so $g^{-1} \in H$ so

$g^{-1}h \in H$, so multiply across by g.

$h = gg^{-1}h \in gH$ so $H \subset gH$

$H \subset gH \subset H$ so $gH = H$.

In general

$g_1 H = g_2 H$

$\iff g_2^{-1} g_1 \in H$

If $g_1 H = g_2 H$, multiply across by g_2^{-1}.

$(g_2^{-1} g_1) H = g_2^{-1} g_2 H = 1 \cdot H = H$

So $g_2^{-1} g_1 = H \iff g_2^{-1} g_1 \in H$

So $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H$.

$[Hg_1 = Hg_2 \,,\; Hg_1 g_2^{-1} = H \iff g_1 g_2^{-1} \in H]$ ← for right cosets.

MATH 7202

17-01-17

Prop

G group, $H \subset G$ subgroup.

Let $\alpha, \beta \in G$

Then either $\alpha H = \beta H$

or $\alpha H \cap \beta H = \phi$

i.e. two cosets are either identical or have empty intersection.

Proof

Suppose that $\alpha H \cap \beta H \neq \phi$

Write $\alpha h_1 = \beta h_2$, $h_i \in H$

$\beta^{-1}\alpha = h_2 h_1^{-1} \in H$

If $\alpha H \cap \beta H \neq \emptyset$ then $\beta^{-1}\alpha \in H$.

So by the rule of equality $\alpha H = \beta H$ □.

Theorem (Lagrange)

Let G be a finite group, with $H \subset G$ a subgroup.

Then $|H|$ divides $|G|$ exactly.

Proof

List the distinct left cosets of H.

$g_1 H, g_2 H, \dots, g_m H$

so $g_i H \cap g_j H = \emptyset$ $i \neq j$

Every $g \in G$ belongs to some coset

$G = g_1 H \sqcup g_2 H \sqcup \dots \sqcup g_m H$ where $\sqcup$ = disjoint union.

So $|G| = \sum_{i=1}^{m} |g_i H|$.

However $|g_i H| = |H|$

Consider $H \mapsto g_i H$ ($h \mapsto g_i h$) which is bijective

with inverse $g_i H \mapsto H$ ($g_i h \mapsto h$).

So $|G| = m|H|$

where m = no. of distinct cosets. □

MATH 7202

20-01-17

G is a finite group, H a subgroup.
List distinct cosets gH: $g_1H, g_2H, \dots, g_kH$.
"distinct" $\Rightarrow$ $g_iH \cap g_jH = \emptyset$ if $i \neq j$.

Every $g \in G$ belongs to some coset (gH),
so $G = \bigcup_{i=1}^{k} g_iH$ and $|G| = \sum_{i=1}^{k} |g_iH|$
(There is no double counting due to cosets being distinct.)

Observe $|g_iH| = |H|$
$\tau_i : H \to g_iH$
$\tau_i(h) = g_ih$
τ_i injective: (surjective by definition)
$\tau_i(h_1) = \tau_i(h_2)$
$\Rightarrow g_ih_1 = g_ih_2$
$\Rightarrow g_i^{-1}g_ih_1 = g_i^{-1}g_ih_2 \Rightarrow h_1 = h_2$

$|G| = k|H|$
k = no. of distinct cosets
ie. $k = |G/H|$
So we get

Prop
$|G| = |G/H||H|$
or $|G/H| = |G|/|H|$

Lagranges Thm ✓

Corollarly "Cauchy's Thm"
Let G be a finite group and $g \in G$.
Then $\mathrm{ord}(g)$ divides $|G|$ exactly.

Proof

If $n = \mathrm{ord}(g)$ then $\{1, g, g^2, \ldots, g^{n-1}\}$ is a subgroup of G $(\cong C_n)$.
Its cardinal is n.
So n divides $|G|$ by Lagrange. $\square$

Prop

Let $h : G \to H$ be a homomorphism (G, H finite groups).
Let $g \in G$, so $h(g) \in H$.
Then $\mathrm{ord}(h(g))$ divides both $|G|$ and $|H|$.

Proof

$\mathrm{ord}(h(g))$ divides $|H|$ by "Cauchy".
Suppose $n = \mathrm{ord}(g)$ so n divides $|G|$ by "Cauchy".
$g^n = 1$
$\Rightarrow h(g^n) = 1$ but also $h(g^n) = h(g)^n$ as h is a homomorphism.
So $h(g)^n = 1$
Put $k = \mathrm{ord}(h(g))$, so $h(g)^k = 1$.
By minimality of k we have $k \leq n$.

Write $n = qk + r$ where $0 \leq r < k$
Then $r = 0$, otherwise $(hg)^n = (h(g)^k)^q h(g)^r = h(g)^r$
If $0 < r < k$ we get a contradiction
(contradicting minimality of k).
So $k = \mathrm{ord}(h(g))$, $k \mid n$.
Also n divides $|G|$.
So $\mathrm{ord}(h(g))$ divides $|G|$. $\square$

MATH 7202

20-01-17

We will consider homomorphisms $\varphi : C_n \mapsto H$
where is some finite group.

$C_n = \{1, z, z^2, \ldots, z^{n-1}\}$, $\text{ord}(z) = n$

<u>Important principle</u>

$\varphi : C_n \mapsto H$ homomorphism

φ is completely determined by the value $\varphi(z) \in H$.

Observe $\varphi(1) = 1$ (no choice!)

Suppose $\varphi(z) = h \in H$ (choice!)

Having chosen h / then have no further choice.

$$\varphi(z^2) = \varphi(z)\varphi(z) = h^2$$

$$\varphi(z^3) = \varphi(z^2)\varphi(z) = h^2 \cdot h = h^3$$

So we must have $\varphi(z^r) = h^r$ once we've chosen $\varphi(z) = h$.

The basic question: "What are the possible choices for $\varphi(z)$?"

<u>Example</u>

$\varphi : C_2 \mapsto C_{12}$ (homomorphism)

$C_3 = \{1, z, z^2\}$, $z^3 = 1$

$C_{12} = \{1, x, x^2, \ldots, x^{11}\}$, $x^{12} = 1$

$\text{ord}(1) = 1$, $\text{ord}(x) = 12$, $\text{ord}(x^2) = 6$, $\text{ord}(x^3) = 4$

$\text{ord}(x^4) = 3$, $\text{ord}(x^5) = 12$, $\text{ord}(x^6) = 2$, $\text{ord}(x^7) = 12$

$\text{ord}(x^8) = 3$, $\text{ord}(x^9) = 4$, $\text{ord}(x^{10}) = 6$, $\text{ord}(x^{11}) = 12$

We want $\varphi : C_3 \mapsto C_{12}$ (homomorphism). What are the possible values of $\varphi(z)$?

$\varphi(z) = 1$ is okay.

This is a trivial homomorphism

$\varphi : G \mapsto H$ $\varphi(g) = 1$ $\forall g \in G$.

$\varphi(z) = x$ forbidden as $12 \nmid 3$.

$\varphi(z) = x^2$ forbidden as $6 \nmid 3$.

$\varphi(z) = x^3$ " " $4 \nmid 3$

$\varphi(z) = x^4$ allowed! $[\varphi(1) = 1,\ \varphi(z) = x^4,\ \varphi(z^2) = x^8]$.

$\varphi(z) = x^5$ forbidden

$\varphi(z) = x^6$ "

$\varphi(z) = x^7$ "

$\varphi(z) = x^8$ allowed! $[\tilde{\varphi}(1) = 1,\ \tilde{\varphi}(z) = x^8,\ \tilde{\varphi}(z^2) = x^4]$.

$\varphi(z) = x^9$ forbidden.

$\varphi(z) = x^{10}$ "

$\varphi(z) = x^{11}$ "

Conclusion

There are precisely three homomorphisms $C_3 \mapsto C_{12}$:

0). $1 \to 1$, $z \to 1$, $z^2 \to 1$.

1). $1 \to 1$, $z \to x^4$, $z^2 \to x^8$

2). $1 \to 1$, $z \to x^8$, $z^2 \to x^4$

Particularly Important Example

$\varphi : C_n \mapsto C_n$

$C_n = \{1, x, \dots, x^{n-1}\}$

Here there are no restrictions on where I can send x. This is because if I send $x \to x^a$ $\mathrm{ord}(x^a)$ certainly divides n.

Def

Let $0 \le a \le n-1$.

Define $\varphi_a : C_n \mapsto C_n$ by $\varphi_a(x^r) = x^{ar}$.

So $\varphi_a(x) = x^a$

Prop :

$\varphi_a : C_n \mapsto C_n$ is a homomorphism

MATH 7202

20-01-17

Proof

$\varphi_a(x^r) = x^r$

$\varphi_a(x^r \cdot x^s) = \varphi_a(x^{r+s}) = x^{a(r+s)}$

$= x^{ar} x^{as} = \varphi_a(x^r)\varphi_a(x^s)$

$\varphi_a(1) = \varphi_a(x^0) = x^{a\times 0} = x^0 = 1.$

$\square$

Prop

There are precisely n homomorphisms $\varphi: C_n \mapsto C_n$ namely $(\varphi_a)_{0 \le a \le n-1}$.

$C_4 \mapsto C_4$, there are 4 homomorphisms

$C_4 = \{1, x, x^2, x^3\}$

$\varphi_0(x) = 1$ (trivial) $\varphi_0(1) = \varphi_0(x) = \varphi_0(x^2) = \varphi_0(x^3)$

$\varphi_1(x) = x$ (identity) $\varphi_1(1) = 1$, $\varphi_1(x) = x$, $\varphi_1(x^2) = x^2$, $\varphi_1(x^3 = x^3$

$\varphi_2(x) = x^2$ $\varphi_2(1) = 1$, $\varphi_2(x) = x^2$, $\varphi_2(x^2) = 1$, $\varphi_2(x^3) = x^2$

$\varphi_3(x) = x^3$ $\varphi_3(1) = 1$, $\varphi_3(x) = x^3$, $\varphi_3(x^2) = x^2$, $\varphi_3(x^3) = x$

φ_1 and φ_3 are bijective, φ_2 is not bijective.

$C_6 \mapsto C_6$, $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$

$\varphi_0(x) = 1$ (trivial) $\varphi_0(x^r) = 1$

$\varphi_1(x) = x$ (Id. bijective) $\varphi_1(x^r) = x^r$

$\varphi_2(x) = x^2$ (not bijective) $\varphi_2(1) = 1$, $\varphi_2(x) = x^2$, $\varphi_2(x^2) = x^4$

$\varphi_2(x^3) = 1$, $\varphi_2(x^4) = x^2$, $\varphi_2(x^5) = x^4$

$\varphi_3(x) = x^3$, $\varphi_3(1) = 1$, $\varphi_3(x) = x^3$, $\varphi_4(x^2) = 1$, ... not bijective

$\varphi_4(x) = x^4$, $\varphi_4(1) = 1$, $\varphi_4(x) = x^4$, $\varphi_4(x^2) = x^2$, $\varphi_4(x^3) = 1$, ... not bijective.

$\varphi_5(x) = x^5$, $\varphi_5(1) = 1$, $\varphi_5(x) = x^5$, $\varphi_5(x^2) = x^4$, $\varphi_5(x^3) = x^3$,

$\varphi_5(x^4) = x^2$, $\varphi_5(x^5) = x$ so bijective

Question: When is $\varphi_a : C_n \mapsto C_n$ bijective? $0 \le a \le n-1$

Theorem

$\varphi_a : C_n \mapsto C_n$ is bijective $\Leftrightarrow$ a is coprime to n.

Proof

$\varphi_a : C_n \mapsto C_n$

C_n is finite so φ_a bijective $\Leftrightarrow$ φ_a surjective.

φ_a surjective precisely when $\operatorname{ord}(x^a) = n$.

$$\operatorname{ord}(x^a) = \frac{n}{HCF(a,n)}$$

$$\begin{aligned}\varphi_a \text{ bijective} &\Leftrightarrow HCF(a,n) = 1 \\ &\Leftrightarrow a, n \text{ are coprime. } \square\end{aligned}$$

Automorphism of a group

Let G be a group.

By an automorphism of G we mean a homomorphism $\alpha : G \mapsto G$ st. α is bijective.

We've already shown that if $\alpha : G \mapsto G$ is auto. then $\alpha^{-1} : G \mapsto G$ is also a homomorphism and so also an automorphism.

Def

$Aut(G) = \{\alpha : G \mapsto G \mid \alpha \text{ is an automorphism}\}$

Theorem

If G is a group then $Aut(G)$ is (naturally) a group in which the group operation is composition.

Proof

Let $\alpha, \beta \in Aut(G)$.

First show that $\alpha \circ \beta : G \mapsto G$ is

(i) a homomorphism, (ii) bijective.

MATH 7202

20-01-17

(i) homomorphism

$$(\alpha\circ\beta)(xy) = \alpha(\beta(xy)) \qquad , \quad x,y \in G$$
$$= \alpha[\beta(x)\beta(y)]$$
$$= \alpha(\beta(x))\,\alpha(\beta(y))$$
$$= (\alpha\circ\beta)(x)\,(\alpha\circ\beta)(y)$$

So $\alpha\circ\beta$ is a homomorphism.

(ii) α, β bijective $\Rightarrow$ $\alpha\circ\beta$ bijective (MATH1201)

So now we have

$$\circ : Aut(G) \times Aut(G) \mapsto Aut(G)$$
$$(\alpha,\beta) \longrightarrow (\alpha\beta)$$

This is the group operation (composition is always associative).

$Id : G \mapsto G$, $Id(x) = x$

Clearly have $\alpha\circ Id = \alpha = Id\circ\alpha$, so we have an identity.

Inverses: If $\alpha \in Aut(G)$ then $\alpha^{-1} \in Aut(G)$ (as above)

$\square$.

Examples

(i) $Aut(C_3) \cong ?$ $\quad C_3 = \{1, x, x^2\}$

$$Aut(C_3) = \{\varphi_a : C_3 \mapsto C_3 \mid a \text{ coprime to } 3\}$$
$$= \{\varphi_1, \varphi_2\}$$

$\varphi_1 = Id$, $\varphi_2(x) = x^2$ $\quad (\tau = \varphi_2)$

So C_3 has precisely 2 automorphisms.

$Id : C_3 \mapsto C_3$, $1 \to 1$, $x \to x$, $x^2 \to x^2$

$\tau : C_3 \mapsto C_3$, $1 \to 1$, $x \to x^2$, $x^2 \to x$

note $\tau\circ\tau = Id$

[Here τ corresponds to complex conjugation, $\omega \to \omega^2$]

(ii) $Aut(C_5) \cong$?

$C_5 = \{1, x, x^2, x^3, x^4, x^5\}$

$Aut(C_5) = \{\varphi_a : C_5 \mapsto C_5 \mid a \text{ coprime to } 5\}$

$= \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$

$\varphi_1(x) = x \quad (Id)$

$\varphi_2(x) = x^2$

$\varphi_3(x) = x^3$

$\varphi_4(x) = x^4$

$(\varphi_2 \circ \varphi_2)(x) = \varphi_2(\varphi_2(x))$

$= \varphi_2(x^2) = \varphi_2(x)^2 = (x^2)^2 = x^4$

$\Rightarrow \varphi_2{}^2 = \varphi_4$

$\varphi_2{}^3(x) = \varphi_2(\varphi_2{}^2(x)) = \varphi_2(x^4)$

$= x^8 = x^3$

$\Rightarrow \varphi_2{}^3 = \varphi_3$

$\varphi_2{}^4 = \varphi_2(\varphi_2{}^3(x)) = \varphi_2(x^3) = x^6 = 1$

$\Rightarrow \varphi_2{}^4 = Id = \varphi_1$

So $Aut\ C_5 \cong C_4 = \{1, \varphi_2, \varphi_2{}^2, \varphi_2{}^2\}$

$Aut\ C_8 \cong$? $\quad C_8 = \{1, x, x^2, x^3, x^4, x^5, x^6, x^7\}$

$Aut(C_8) = \{\varphi_a : C_8 \mapsto C_8 \mid a \text{ is coprime to } 8)$

$= \{\varphi_1, \varphi_3, \varphi_5, \varphi_7\}$

$\varphi_3{}^2(x) = \varphi_3(x^3) = x^9 = x \Rightarrow \varphi_3{}^2 = Id$

$\varphi_5{}^2(x) = \varphi_5(x^5) = x^{25} = x \Rightarrow \varphi_5{}^2 = Id$

$\varphi_7{}^2(x) = \varphi_7(x^7) = x^{49} = x \Rightarrow \varphi_7{}^2 = Id$

$\circ$	Id	φ_3	φ_5	φ_7
Id	Id	φ_3	φ_5	φ_7
φ_3	φ_3	Id	φ_7	φ_5
φ_5	φ_5	φ_7	Id	φ_3
φ_7	φ_7	φ_5	φ_3	Id

So $Aut(C_8) = \underset{\varphi_3}{C_2} \times \underset{\varphi_5}{C_2}$

MATH 7202

24-01-17

General Result: (Proof will follow eventually)

If p is prime, $Aut(C_p) \cong C_{p-1}$

You can check this for small p.

We can assume this (but state what we are doing).

Example

$Aut(C_{11}) \cong C_{10}$

$C_{11} = \{1, x, \dots, x^{10}\}$

$Aut(C_{11}) = \{\varphi_a : 1 \le a \le 10, a \text{ coprime to } 11\}$

$Aut(C_{11}) = \{Id, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8, \varphi_9, \varphi_{10}\}$

Put $\alpha = \varphi_2$

$$\begin{array}{cccccccccc} 1, & \alpha, & \alpha^2, & \alpha^3, & \alpha^4, & \alpha^5, & \alpha^6, & \alpha^7, & \alpha^8, & \alpha^9 \\ \| & \| & \| & \| & \| & \| & \| & \| & \| & \| \\ 1 & \varphi_2 & \varphi_4 & \varphi_8 & \varphi_5 & \varphi_{10} & \varphi_9 & \varphi_7 & \varphi_3 & \varphi_6 \end{array}$$

So $ord(\alpha) = 10$

$\Rightarrow Aut(C_{11}) \cong C_{10}$

Example

$Aut(C_7) \cong C_6$

$C_7 = \{1, x, \dots, x^6\}$

$Aut(C_7) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}$

Let $\alpha = \varphi_3$

$\alpha^2 = \varphi_2, \ \alpha^3 = \varphi_6, \ \alpha^4 = \varphi_4, \ \alpha^5 = \varphi_5$

$Aut(C_7) = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 : \alpha = \varphi_3\}$

Unsolved problem

For which primes p is it true that φ_2 generates $Aut(C_p)$

$C_3 = \{1, x, x^2 \mid x^3 = 1\}$
$C_2 = \{1, y \mid y^2 = 1\}$

$C_3 \times C_2 = \{(1,1), (x,1), (x^2,1), (1,y), (x,y), (x^2,y)\}$

$(x^a, y^b)(x^c, y^d) = (x^{a+c}, y^{b+d}) = (x^{c+a}, y^{d+b}) = (x^c, y^d)(x^a, y^b)$
So $C_3 \times C_2$ is an abelian group.

Write $X = (x,1)$, $Y = (1,y)$
So $C_3 \times C_2 = \{1, X, X^2, Y, XY, X^2Y\}$
$X^3 = 1, \quad Y^2 = 1, \quad YX = XY$

$D_6 = \{1, X, X^2, Y, XY, X^2Y\}$
$X^3 = 1, \quad Y^2 = 1, \quad YX = X^2Y$

For English Lit. these are the same!
But they are wrong as $C_3 \times C_2 \neq D_6$!!

Direct product of two groups
$G = (G, \cdot, 1)$, $H = (H, *, 1)$
$G \times H = (G \times H, \square, (1,1))$ where $(g_1, h_1) \square (g_2, h_2) = (g_1 \cdot g_2, h_1 * h_2)$
This is a group operation with $(1,1)$ as the identity.
$(g,h)^{-1} = (g^{-1}, h^{-1})$
$(1,h) \square (g,1) = (g,1) \square (1,h) = (g,h)$.

Generalisation
Semi-direct product
$K \rtimes_c Q$
Here K is a group, Q is a group.
$c : Q \longrightarrow \mathrm{Aut}(K)$ is a homomorphism.

MATH 7202

24-01-17

Def

As a set, $K \rtimes_c Q = K \times Q$

$= \{(k,q) : k \in K, q \in Q\}$

Multiplication:

$(k_1, q_1) \cdot (k_2, q_2) = (k_1 c(q_1)(k_2), q_1 q_2)$

This makes sense because

$c : Q \mapsto Aut(K)$

so $c(q_1) : K \mapsto K$ automorphism

so $c(q_1)(k_2) \in K$

As identity we take $1 \in (1,1)$.

Describe D_6 as a semidirect product.

$D_6 = C_3 \rtimes_c C_2$

$C_3 = \{1, x, x^2 \mid x^3 = 1\}$

$C_2 = \{1, y \mid y^2 = 1\}$

How about $c : C_2 \mapsto Aut(C_3)$

Last time we showed $Aut(C_3) \cong C_2 = \{1, \tau\}$

where $\tau(1) = 1$, $\tau(x) = x^2$, $\tau(x^2) = x$.

Let $c : C_2 \mapsto Aut(C_3)$ be $c(y) = \tau$

Multiplication on $C_3 \rtimes_c C_2$ is given by:

$(1, y) * (x, 1) = (1 \cdot c(y)(x), y \cdot 1)$

$c(y)(x) = \tau(x) = x^2 \Rightarrow (1,y) * (x,1) = (x^2, y)$

So now if we write $X = (x,1)$ and $Y (1,y)$ then

$Y \cdot X = (x^2, y) = X^2 Y$

This is the characteristic eqn. for D_6.

$D_6 \cong C_3 \rtimes_c C_2$

where $c : C_2 \mapsto Aut(C_3)$, $c(y) = x$

There is another possibility for c.

$C_2 = \{1, y\}$, $Aut(C_3) = \{1, \tau\}$.

Take c to be the trivial homomorphism

$c(1) = Id$, $c(y) = Id$.

Now $c(y)(x) = x$.

If we do the corresponding multiplication,

$$(1, y) * (x, 1) = (1 \cdot c(y)(x), y \cdot 1)$$
$$= (x, y) = (x, 1) * (1, y)$$

So taking c to be trivial,

write $X = (x, 1)$, $Y = (1, y)$

we get $YX = (x, y) = XY$

which is $C_3 \times C_2$.

So for $C_3 \rtimes_c C_2$ there are two possibilities for c.

1). Trivial case : $c(y) = Id$ which gives

$C_3 \rtimes_c C_2 = C_3 \times C_2$ which is abelian

2). Non-trivial case : $c(y) = \tau$ which gives

$C_3 \rtimes_c C_2 \cong D_6$

This construction gives groups you have not yet seen

$G(21) = G(7, 3)$

$C_7 \rtimes_c C_3$

$C_7 = \{1, x, x^2, x^3, x^4, x^5, x^6\}$, $x^7 = 1$, $C_3 = \{1, y, y^2\}$ $y^3 = 1$

$c : C_3 \mapsto Aut(C_7) \cong C_6 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ where $\alpha(x) = x^3$

$ord(\alpha^2) = 3$, $\alpha^2(x) = x^2$ $\quad (\alpha^2(x) = \alpha(\alpha(x)) = (x^3)^3 = x^9 = x^2)$

The multiplication $C_7 \rtimes_c C_3$ looks like

$$(1, y) * (x, 1) = (1 \cdot c(y)(x), y \cdot 1) = (x^2, y)$$

Write $X = (x, 1)$, $Y = (1, y)$ then $X^7 = 1$, $Y^3 = 1$

$YX = X^2 Y$

$G(7, 3) = \langle X, Y \mid X^7 = 1, Y^3 = 1, YX = X^2 Y \rangle$.

MATH 7202

27-01-17

Normal Subgroup

$D_6 = \{1, x, x^2, y, xy, x^2y\}$ $\quad x^3 = 1,\ y^2 = 1,\ yx = x^2y$

Put $K = \{1, x, x^2\}$, $Q = \{1, y\}$
Both K and Q are subgroups.

$G/K = \{gK : g \in G\}$ $\quad [G = D_6]$
$K\backslash G = \{Kg : g \in G\}$

$G/Q = \{gQ : g \in G\}$
$Q\backslash G = \{Qg : g \in G\}$

$\underline{G/K}$

$1 \cdot K = \{1, x, x^2\}$
$x \cdot K = \{x, x^2, 1\}$
$x^2 \cdot K = \{x^2, 1, x\}$
these have the same elements

$y \cdot K = \{y, yx, yx^2\} = \{y, x^2y, xy\}$
$xy \cdot K = \{xy, y, x^2y\}$
$x^2y \cdot K = \{x^2y, xy, y\}$
these have the same elements

So G/K has two elements
$G/K = \{\{1, x, x^2\}, \{y, xy, x^2y\}\}$

$\underline{K\backslash G}$

$K \cdot 1 = \{1, x, x^2\}$
$K \cdot x = \{x, x^2, 1\}$
$K \cdot x^2 = \{x^2, 1, x\}$
these have the same elements

$K \cdot y = \{y, xy, x^2y\}$
$K \cdot xy = \{xy, x^2y, y\}$
$K \cdot x^2y = \{x^2y, y, xy\}$
these have the same elements.

So $K\backslash G = \{\{1, x, x^2\}, \{y, xy, x^2y\}\}$
In this case $G/K = K\backslash G$

$\underline{G/Q}$

$1 \cdot Q = \{1, y\} \quad = \quad y \cdot Q = \{y, 1\}$
$x \cdot Q = \{x, xy\} \quad = \quad xy \cdot Q = \{xy, x\}$
$x^2 \cdot Q = \{x^2, x^2y\} \quad = \quad x^2y \cdot Q = \{x^2y, x^2\}$

So $G/Q = \{\{1, y\}, \{x, xy\}, \{x^2, x^2y\}\}$
(it has three elements)

$\underline{Q \backslash G}$

$Q \cdot 1 = \{1, y\}$
$Q \cdot x = \{x, yx\} = \{x, x^2y\}$
$Q \cdot x^2 = \{x^2, yx^2\} = \{x^2, xy\}$
$Q \cdot y = \{y, 1\}$
$Q \cdot xy = \{xy, x^2\}$
$Q \cdot x^2y = \{x^2y, x\}$

So $Q \backslash G = \{\{1, y\}, \{x, x^2y\}, \{x^2, xy\}\}$
So $Q \backslash G \neq G/Q$

Def
Let K be a subgroup of G.
We say that K is <u>normal</u> in G when for each $g \in G$, $gK = Kg$.

"Normal" is terrible terminology as it is very rare!

In $D_6 = \{1, x, x^2, y, xy, x^2y\}$
$K = \{1, x, x^2\}$ is <u>normal</u> in D_6.
$Q = \{1, y\}$ is <u>not normal</u> in D_6.

When K is a normal subgroup of G we write '$K \triangleleft G$'.

MATH 7202

27-01-17

Normality can be expressed in a number of different ways:

(i) $K \lhd G \Leftrightarrow \forall g \in G \quad gK = Kg$ (Definition above)

(ii) $K \lhd G \Leftrightarrow \forall k \in K, \forall g \in G, gkg^{-1} \in K$

Prop

In the above $i \Leftrightarrow ii$.

Proof Assume $gK = Kg \quad \forall g \in G$.

Let $k \in K \quad gK = kg = Kg$

If $k \in K \ \exists k_1 \in K$ s.t. $gk = k_1 g$

so $gkg^{-1} = k_1 \in K$ so $i \Rightarrow ii$

Assume that for $g \in G$, $k \in K$, $gkg^{-1} \in K$

i.e. $\forall g \in G \ \forall k \in K \ \exists k_1 \in K$.

$gk = k_1 g$

$gkK = k_1 gK$

$gK = k_1 gK$

$Kg = \{kg : k \in K\}$

$1 \cdot Kg = Kg$

$g \cdot (g^{-1}Kg) = Kg$

$\forall k \in K \ g^{-1}kg \in K \Rightarrow g^{-1}k(g^{-1})^{-1} \in K \Rightarrow \exists k_1 \in K$ s.t. $g^{-1}kg = k_1$

$g(g^{-1}kg) = gk_1 \in gK$

So $gK \subset Kg$

By symmetry $Kg \subset gK$

so (ii) $\Rightarrow$ (i)

$\square$

Now suppose $K \lhd G$ and let $g \in G$.
So if

$$k \in K \Rightarrow gkg^{-1} \in K \quad \forall g \in G \qquad \left[\begin{array}{l} gK = Kg \\ \Rightarrow gKg^{-1} = K \end{array}\right]$$

So suppose $K \lhd G$ and consider the mapping

$$g \mapsto \{k \mapsto gkg^{-1}\}$$

If $g \in G$ we write

$$c_g(k) = gkg^{-1}.$$

<u>Prop</u>

If $K \lhd G$ and $g \in G$, then the mapping

$$c_g : K \mapsto K \quad , \quad c_g(k) = gkg^{-1}$$

is an automorphism of K.

<u>Proof</u>

Need to show

(i) c_g is a homomorphism

(ii) c_g is bijective.

(i) $c_g(k_1k_2) = g(k_1k_2)g^{-1} = gk_1g^{-1}gk_2g^{-1}$

(inserted cancelling pair $g^{-1}g$)

so $c_g(k_1k_2) = c_g(k_1)c_g(k_2)$

so c_g is a homomorphism.

(ii) To show c_g is bijective, notice that c_g^{-1} is defined:

$$c_g^{-1}(k') = g^{-1}k'g \qquad [g = (g^{-1})^{-1}]$$

$$\begin{aligned}(c_g \circ c_g^{-1})(k) &= c_g(g^{-1}kg) \\ &= gg^{-1}kgg^{-1} \\ &= 1 \cdot k \cdot 1 = k\end{aligned}$$

so $c_g \circ c_g^{-1} = Id$, by symmetry $c_g^{-1} \circ c_g = Id$

so c_g is a bijection.

$\therefore$ c_g is an automorphism. $\square$

To summarise, if $K \lhd G$, each $g \in G$ gives an automorphism $c_g \in Aut(K)$.

Now consider the mapping

$$c : G \mapsto Aut(K)$$
$$g \mapsto c_g$$

Prop

If $K \lhd G$ then $c : G \mapsto Aut(K)$ $\quad (c_g(k) = gkg^{-1})$ is a homomorphism.

Proof

Need to show $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$.

$$\begin{aligned} c_{g_1 g_2}(k) &= g_1 g_2 k (g_1 g_2)^{-1} \\ &= g_1 (g_2 k g_2^{-1}) g_1^{-1} \\ &= c_{g_1}(g_2 k g_2^{-1}) \\ &= c_{g_1}(c_{g_2}(k)) \\ &= (c_{g_1} \circ c_{g_2})(k) \end{aligned}$$

true for all $k \in K$. $\square$

[This is in all standard texts e.g. { Ledermann & Weir, Lang's Algebra } or any "Intro to abstract algebra".]

If $K \lhd G$ we get a homomorphism

$$c : G \mapsto Aut(K), \quad c_g(k) = gkg^{-1}.$$

c is called the conjugation map.

c_g is called congugation by g.

If $Q \subset G$ is a subgroup we still get a homomorphisms $c : Q \mapsto Aut(K)$ by restricting domain to Q.

Semidirect products (Abstract Form)

Initial data

K a group, Q a group
$c : Q \mapsto Aut(K)$ is a homomorphism.

Construct $K \rtimes_c Q$ as follows

As a set:

? $K \rtimes_c Q = K \times Q$

Multiplication

$(k_1 q_1) \cdot (k_2 q_2) = (k_1 c(q_1)(k_2), q_1 q_2)$

where $c(q_1) : K \mapsto K$ so $c(q_1)(k_2) \in K$

This multiplication is associative (see next weeks homework!)

The identity is $(1,1)$.

Finding $(k,q)^{-1}$ is also on the homework.

In multiplying in $K \rtimes_c Q$ there are essentially 4 distinct cases:

1). $(k_1, 1)(k_2, 1) = (k_1 k_2, 1)$

2). $(k,1)\cdot(1,q) = (k,q)$

3). $(1, q_1)(1, q_2) = (1, q_1 q_2)$

4). $(1,q)(k,1) = (c(q)(k), q)$

Crucial case!

1): $(k_1, 1)\cdot(k_2, 1) = (k_1 \cdot c(1)(k_2), 1 \cdot 1) = (k_1 k_2, 1)$

as $c : Q \mapsto Aut(K)$ is a homomorphism

so $c(1) = Id \Rightarrow c(1)(k_2) = k_2$

2).: $(k,1)\cdot(1,q) = (k \cdot c(1)(1), 1\cdot q) = (k \cdot 1, q) = (k,q)$

3).: $(1,q_1)\cdot(1,q_2) = (1 \cdot c(q_1)(1), q_1 q_2) = (1, q_1 q_2)$

as $c(q_1)$ is a homomorphism so $c(q_1)(1) = 1$

MATH 7202

27-01-17

Semidirect Products (Concrete Form)

Given a group G how can we recognise if G is a semidirect product?

Recognition Criterion

Let G be a finite group with subgroups K, Q of G.

(i) $K \lhd G$

(ii) $K \cap Q = \{1\}$

(iii) $|G| = |K||Q|$

Then $G \cong K \rtimes_c Q$

where $c : Q \mapsto Aut(K)$, $c_q(k) = qkq^{-1}$

is the conjugation map.

Proof

Define $\Phi : K \rtimes_c Q \mapsto G$

by $\Phi(k, q) = kq$ (mult. in G)

Φ is a well defined mapping on sets.

I claim that Φ is a homomorphism $\Phi : K \rtimes_c Q \mapsto G$

$$\begin{aligned}\Phi((k_1, q_1)\cdot(k_2, q_2)) &= \Phi(k_1 c(q_1)(k_2), q_1 q_2)\\ &= \Phi(k_1 q_1 k_2 q_1^{-1}, q_1 q_2)\\ &= k_1 q_1 k_2 q_1^{-1} q_1 q_2\\ &= k_1 q_1 k_2 q_2\\ &= \Phi(k_1, q_1)\Phi(k_2, q_2)\end{aligned}$$

so Φ is a homomorphism.

Claim that Φ is injective.

Suppose $\Phi(k_1, q_1) = \Phi(k_2, q_2)$

$$k_1 q_1 = k_2 q_2$$

so $k_2^{-1} k_1 = q_2 q_1^{-1}$

Now $k_2^{-1} k_1 \in K$, $q_2 q_1^{-1} \in Q$

so $k_2^{-1} k_1 \in K \cap Q = \{1\}$

so $k_2^{-1} k_1 = 1 \Rightarrow k_1 = k_2$

and $q_2 q_1^{-1} = 1 \Rightarrow q_1 = q_2$

So $\Phi(k_1, q_1) = \Phi(k_2, q_2) \Rightarrow (k_1, q_1) = (k_2, q_2)$

So now we have an injective homomorphism

$\Phi : K \rtimes_c Q \hookrightarrow G.$

The cardinal of the LHS $= |K||Q|$

" " " " RHS $= |G|$

By hypothesis $|G| = |K||Q|$

So Φ is bijective because G is finite. $\square$

It turns out that many groups of "small order" are semi-direct products.

<u>Classification of groups of order $2p$</u>

If p is an odd prime, then we're going to show that if $|G| = 2p$ then

<u>either</u> $G \cong C_{2p}$ $(\cong C_p \times C_2)$

<u>or</u> $G \cong D_{2p}$

<u>Theorem</u>

Let G be a finite group with the property that $\forall x \in G$ $x^2 = 1$, then

(i) G is abelian

(ii) $G \cong \underbrace{C_2 \times C_2 \times \ldots \times C_2}_{n \text{ groups}}$ for some n

(iii) $|G| = 2^n$ for some n.

<u>Proof</u>

(i) Let $x, y \in G$

$x^2 = 1$, $y^2 = 1$, $(xy)^2 = 1$

$(xy)^2 = 1 \Rightarrow (xy)^{-1} = xy$

But $(xy)^{-1} = y^{-1}x^{-1}$

$x^2 = 1 \Rightarrow x^{-1} = x$

$y^2 = 1 \Rightarrow y^{-1} = y$

so $(xy)^{-1} = yx$ so $yx = xy$

True for all $x, y \in G$,
$yx = xy \Rightarrow G$ is abelian.

(ii) Since G is abelian we can write it additively
i.e. $\begin{cases} x+y & \text{instead of } xy \\ 0 & \text{" " } 1 \\ 2x & \text{" " } x^2 \end{cases}$

So $x^2 = 1$ translates to $2x = 0 \Rightarrow x + x = 0$.
Can regard G as a vector space over $\mathbb{F}_2 = \{0, 1\}$
(field with two elements)
G is finite so f.g is a vector space.

Apply Basis Theorem.
$$G \cong \underbrace{\mathbb{F}_2 \oplus \dots \oplus \mathbb{F}_2}_{n}$$

So $|G| = 2^n$ for some n.

Now translate back to multiplication.
$\mathbb{F}_2 = \{0, 1\} \cong C_2 = \{1, t\}$
$0 \longmapsto 1$
$1 \longmapsto t$
$$\underbrace{\mathbb{F}_2 \oplus \dots \oplus \mathbb{F}_2}_{n} \cong \underbrace{C_2 \times \dots \times C_2}_{n}$$
$\square$

$|G| = 2p$ $\quad p$ odd
$\Rightarrow \exists x \in G$ s.t. $\mathrm{ord}(x) = p$

MATH 7202

31-01-17

Prop

Let p be prime and G be a group where $|G| = p$.
Then $G \cong C_p$

Proof

If $x \in G$, $x \neq 1$ then $\text{ord}(x) = p$
so $G = \{1, x, x^2, \ldots, x^{p-1}\} \cong C_p$

$\square$

Note that if $|G| = p$, $x \in G$, $x \neq 1 \Rightarrow x$ generates G.

Theorem

If p is an odd prime and $|G| = 2p$, then
either (i) $G \cong C_{2p} \cong C_p \times C_p$
or (ii) $G \cong D_{2p}$.

Prop

Let p be an odd prime and let
$\alpha : C_p \mapsto C_p$ be an automorphism.
If $\alpha^2 = Id$ then
either (i) $\alpha = Id$
or (ii) $\alpha(g) = g^{-1}$ for any $g \in C_p$.

Proof:

Write $C_p = \{1, x, \ldots, x^{p-1}\}$
Consider $z = \alpha(x)\, x$.
Apply α: $\alpha(z) = \alpha^2(x)\alpha(x)$
$= x\,\alpha(x)$
$= \alpha(x)\, x = z$

Two possibilities for z:

a). $z \neq 1$
b). $z = 1$

If a). then z generates C_p, $\alpha(z) = z \Rightarrow \alpha = Id$.
If b). then $\alpha(x)\, x = 1 \Rightarrow \alpha(x) = x^{-1}$.

So if b)., $\alpha(x^r) = x^{-r}$ $\forall r$.

$\square$

Theorem

Let p be an odd prime and G be a group with $|G| = 2p$. Then

I). $\exists\, x \in G$: $ord(x) = p$

II). G has a normal subgroup of order p

III). $\exists\, y \in G$: $ord(y) = 2$

Proof

I). $|G| = 2p$. If $g \in G$ then either

$$\left.\begin{array}{l} \text{(i) } ord(g) = 1 \quad (g = 1) \\ \text{or (ii) } ord(g) = 2 \\ \text{or (iii) } ord(g) = p \\ \text{or (iv) } ord(g) = 2p. \end{array}\right\} \text{Lagrange}$$

If every nontrivial $g \in G$ has $ord(g) = 2$ then $|G| = 2^n$ (last lecture)

Contradiction as p is odd.

So either

a). $\exists\, x \in G$: $ord\, x = p$

or b). $\exists\, z \in G$: $ord\, z = 2p$

If a) we have our element x of order p.

? If b), put $x = z^2$, then $ord(x) = p$

QED (I).

II). Let $x \in G$, $ord(x) = p$.

Put $K = \{1, x, \dots, x^{p-1}\}$, then K is a subgroup of G, $K \cong C_p$.

$|G/K| = 2 = |K \backslash G|$ so $G = K \sqcup gK$ $g \notin K$

also $G = K \sqcup Kg$ $g \notin K$,

so if $g \notin K$ $gK = Kg$ wheras if $g \in K$ then $gK = Kg = K$.

i.e. $\forall g \in G$, $gK = Kg$ so $K \triangleleft G$ QED (II)

III). Let $z \in G$.

Hence $G = K \sqcup zK$.

Claim that $z^2 \in K$.

$G = zG = zK \sqcup z^2K$

Also $G = zK \sqcup K$

So $z^2K = K$ so $z^2 \in K$

$z^2 \in K \cong C_p$ so either

(i) $z^2 = 1$ $\operatorname{ord}(z) = 2$

or (ii) $z^2 \neq 1$ $\operatorname{ord}(z^2) = p$

and $\operatorname{ord}(z) = 2p$, and $\operatorname{ord}(z^p) = 2$

If (i) put $y = z^2$,

if (ii) put $y = z^p$.

Either way $\operatorname{ord}(y) = 2$ QED (III).

□

Corollary

If G is a finite group, $|G| = 2p$, p an odd prime,

then either $G \cong C_{2p} \cong C_p \times C_2$

or $G \cong D_{2p}$.

Proof

By above Thm, G has a normal subgroup K

$|K| = p$, $K \cong C_p$

Also G has a subgroup Q. $|Q| = 2$ namely $Q = \{1, y\}$ where $\operatorname{ord}(y) = 2$.

$K \cap Q = \{1\}$ (2, p coprime).

Apply recognition criterion.

$G \cong K \rtimes_c Q$ (where $c(q)(k) = qkq^{-1}$)

$G \cong C_p \rtimes_c C_2$

$c: C_2 \to \operatorname{Aut}(C_p)$ is a homomorphism

$y^2 = 1 \Rightarrow c(y^2) = \mathrm{Id}.$

Write $K = \{1, x, \dots, x^{p-1}\}$

then either

a). $c(y)(x) = x$

b). $c(y)(x) = x^{-1}$

If a). $yxy^{-1} = x$.

$G = \{1, x, \dots, x^{p-1}, y, xy, \dots, x^{p-1}y\}$

$x^p = 1$, $y^2 = 1$, $yx = xy$

$G \cong C_p \times C_2 \cong C_{2p}$.

If b). $yxy^{-1} = x^{-1} = x^{p-1}$

$G = \{1, x, \dots, x^{p-1}, y, xy, \dots, x^{p-1}y\}$

$x^p = 1$, $y^2 = 1$, $yx = x^{p-1}y$

$G \cong D_{2p}$.

$\square$

$G = C_m \times C_n$

$G \cong C_{mn} \Leftrightarrow m, n$ coprime

If x generates C_m and y generates C_n

m, n coprime $\Rightarrow \operatorname{ord}(x, y) = nm$

$\lvert G\rvert$	Known possibilities	Complete?	$\lvert G\rvert$	Known possibilities	Complete?
1	$\{1\}$	✓	14	$C_{14} \cong C_7 \times C_{12}$, D_{14}	✓
2	C_2	✓	15	$C_{15} \cong C_5 \times C_3$	??
3	C_3	✓	16		
4	$C_4 \cong C_2 \times C_2$	✓	17	C_{17}	✓
5	C_5	✓	18		
6	$C_6 \cong C_3 \times C_2$, D_6	✓	19	C_{19}	✓
7	C_7	✓	20		
8	$C_8 \cong C_4 \times C_2 \cong C_2 \times C_2 \times C_2$, D_8 $Q(8)$	??	21		
9	$C_9 \cong C_3 \times C_3$	??	22	$C_{22} \cong C_{11} \times C_2$, D_{22}	✓
10	$C_{10} \cong C_5 \times C_2$, D_{10}	✓	23	C_{23}	✓
11	C_{11}	✓	24		
12			25		
13	C_{13}	✓	26	$C_{26} \cong C_{13} \times C_2$, D_{26}	✓

MATH 7202

03-02-17

Groups of order $2p$ (p odd prime)

G group, $|G| = 2p$ then

either (i) $G \cong C_{2p} \cong C_p \times C_2$

or (ii) $G \cong D_{2p} \cong C_p \rtimes_h C_2$ (h nontrivial).

Coming soon!

"pq^m - theorem"

If p, q are primes and $q^m < p$ then any group G with $|G| = pq^m$ is a semidirect product

$$G \cong C_p \rtimes_h Q$$

where $|Q| = q^m$ and $h : Q \mapsto Aut(C_p)$ is some homomorphism.

For now we will believe this is true and see what we get.

$G \cong C_p$ ✓

$|G| = 2p$, $G \cong C_{2p}$ or D_{2p}

Briefly consider groups $|G| = 3p$ where p is a prime $(3 < p)$.

Apply "pq^m-theorem" with $q = 3$, $m = 1$, we get $G \cong C_p \rtimes_h C_3$ for some $h : C_3 \mapsto Aut(C_p) \cong C_{p-1}$

e.g. $|G| = 21 = 7 \times 3$

so $G \cong C_7 \rtimes_h C_3$ (by pq^m Thm)

$C_7 = \{1, x, x^2, x^3, x^4, x^5, x^6\}$, $x^7 = 1$

$C_3 = \{1, y, y^2\}$, $y^3 = 1$

How many possibilities for h?

$Aut(C_7) \cong C_6 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$

where $\alpha(x) = x^3$, $ord(\alpha) = 6$

	$\alpha = \varphi_3$,	$\alpha^2 = \varphi_2$ $(= \varphi_9)$,	$\alpha^3 = \varphi_6$,	$\alpha^4 = \varphi_4$,	$\alpha^5 = \varphi_5$,	$\alpha^6 = Id$
ord:	6	3	2	3	6	1

How many homomorphisms

$h: C_3 \mapsto C_6 \cong Aut(C_7)$

$C_3 = \{1, y, y^2\}$ can only have $ord[h(y)] = 1$ or 3

<u>can't</u> have $ord[h(y)] = 2$ or 6

So there are 3 homorphisms

$h_0(y) = Id \quad , \quad h_0(y^2) = Id$

$h_1(y) = \alpha^2 = \varphi_2 \quad , \quad h_1(y^2) = \alpha^4 = \varphi_4$

$h_2(y) = \alpha^4 = \varphi_4 \quad , \quad h_2(y^2) = \alpha^2 = \varphi_2$

For each r get semidirect product

$G(r) = C_7 \rtimes_{h_r} C_3$

Take $r = 0$, $C_7 \rtimes_{h_0} C_3$, $h_0(y) = Id$

$X = (x, 1) \quad , \quad Y = (1, y)$

$X^7 = 1, \quad Y^3 = 1$

$h_0(y)(x) = x$

$yxy^{-1} = x \Rightarrow YXY^{-1} = X$ or $YX = XY$.

So $G(0) = C_7 \times C_3$

Take $r = 1$, $C_7 \rtimes_{h_1} C_3$, $h_1(y) = \alpha^2 = \varphi_2$, $h_1(y)(x) = x^2$

$X = (x, 1) \quad , \quad Y = (1, y) \quad , \quad X^7 = 1 \quad , \quad Y^3 = 1$

$h_1(y)(x) = x^2 \Rightarrow yxy^{-1} = x^2$

so $YX = X^2 Y$

Take $r = 2$, $C_7 \rtimes_{h_2} C_3$, $h_2(y) = \alpha^4 = \varphi_4$, $h_2(y)(x) = x^4$

$X = (x, 1), \quad X^7 = 1, \quad Y = (1, y), \quad Y^3 = 1$

$h_2(y)(x) = x^4 \quad , \quad yxy^{-1} = x^4$

$\Rightarrow YX = X^4 Y$

$$\left[\begin{array}{c} (1, y)(x, 1) = (h_2(y)(x), y) = (x^4, y) = (x^4, 1)(1, y) \\ \Rightarrow YX = X^4 Y \end{array} \right]$$

MATH 7202

03-02-17

So $\begin{cases} G(0) = \langle X, Y \mid X^7=1,\ Y^3=1,\ YX = XY \rangle \\ G(1) = \langle X, Y \mid X^7=1,\ Y^3=1,\ YX = X^2Y \rangle \\ G(2) = \langle X, Y \mid X^7=1,\ Y^3=1,\ YX = X^4Y \rangle \end{cases}$

$G(0)$ is abelian $\cong C_7 \times C_3 \cong C_{21}$

$G(1)$, $G(2)$ nonabelian.

Prop.

$G(2) \cong G(1)$

Proof

Choose alternative generator for C_3, $z = y^2$

$X^7 = 1$, $Z^3 = 1$

Let's do the crucial calculation (using h_2) with z replacing y.

$h_2(z)(x) = z^2(x) = x^2$

$ZX = X^2 Z$

$G(2) \cong G(1)$ $X \mapsto X$, $Y \mapsto Y^2 = Z$ $\square$

So if we believe the "pq^m-Thm" then we get:

Corollary

There are precisely two distinct groups of order 21

(i) $C_{21} \cong C_7 \times C_3$

(ii) $G(21) = \langle X, Y \mid X^7=1,\ Y^3=1,\ YX = X^2Y \rangle = G(7,3)$.

Example

Suppose p, $p-2$ both primes.

Then there is only one group of order $p(p-2)$

namely $C_{p(p-2)} \cong C_p \times C_{p-2}$

Still believe pq^m-Thm.

Take $q = p-2$, $m=1$.

If $|G| = p(p-2)$ then G is a semidirect product

$G \cong C_p \rtimes_h C_{p-2}$ for some $h : C_{p-2} \to \mathrm{Aut}(C_p) = C_{p-1}$

$p-1$ is divisible by 2
So $\frac{p-1}{2} < p-2$

$Aut(C_p) \cong C_{p-1}$ clearly has no element of order $p-2$.
$C_p = \{1, x, \dots, x^{p-1}\}$, $x^p = 1$
$C_{p-2} = \{1, y, \dots, y^{p-3}\}$, $y^{p-2} = 1$
$h: C_{p-2} \to Aut(C_p)$ must have the form $h(y) = Id$.
$h(y)(x) = x$, $YXY^{-1} = X$
$C_p \rtimes_h C_{p-2} = \langle X, Y \mid X^p = 1, Y^{p-2} = 1, YX = XY \rangle$
$\cong C_p \times C_{p-2} \cong C_{p(p-2)}$ ($p, p-2$ coprime)

Examples
1). $p = 5$, $p-2 = 3$
There is only one group of order 15,
namely $C_{15} = C_5 \times C_3$.
2). $p = 7$, $p-2 = 5$
There is only one group of order 35
$C_{35} \cong C_7 \times C_5$
3). $p = 31$, $p-2 = 29$
$\exists$ a unique group of order $31 \times 29 = 899$ $(30+1)(30-1)$
So $C_{899} \cong C_{31} \times C_{29}$

[pronounced seal-off]
Sylow's Thm
p prime, $k \geq 1$ an integer coprime to p.
G finite group with $|G| = kp^m$ $(m \geq 1)$. Then
I). G has at least one subgroup P with $|P| = p^n$.
II). If N_p is the number of subgroups of order p^n then
$N_p \equiv 1 \mod p$.
III). N_p divides $|G|$
IV). If P is a subgroup, $|P| = p^n$.
P' is a subgroup of order p^e $(e \leq n)$ then
$\exists g \in G : gP'g^{-1} \subset P$.

MATH 7202

03-02-17

Let's believe Sylow I and II for now.

Sylow Counting

Example

Suppose $G = pq^m$, p and q both primes, $q^m < p$.
Claim that G has a normal subgroup of order p.
Sylow I with $n=1$ says that G has at least one subgroup K with $|K| = p$.
In particular $K \cong C_p$.

Let N_p be the number of distinct subgroups of order p. Sylow II says that $N_p \equiv 1 \mod p$.

So either $N_p = 1$ or $N_p \geq p+1$.
Claim that when $q^m < p$ we must have $N_p = 1$.
If not, $\exists$ at least $(p+1)$-subgroups
$K_1, K_2, \dots, K_{p+1}$, $|K_i| = p$.
i.e. each $K_i \cong C_p$.
Each K_i has $(p-1)$ elements of order p.
If $i \neq j$, $K_i \cap K_j = \{1\}$, otherwise:
$\exists\ z \in K_i \cap K_j$, $z \neq 1$, so $\mathrm{ord}(z) = p$.
$z \in K_i$ so z generates K_i, $z \in K_j$ so z generates K_j
so $K_i = K_j$. ⨳ contradiction.

So $\exists$ at least $(p+1)(p-1) = p^2 - 1$ elements of order p.
Include identity element $(\mathrm{ord} = 1)$ so G has at least p^2 elements.

$$p^2 \leq |G| = \underset{< p^2}{pq^m}, \quad q^m < p$$

⨳ contradiction.

Conclusion: Let $|G| = pq^m$, p, q prime, $q^m < p$.
Then G has a unique subgroup K, $|K| = p$, $K \cong C_p$.

So assuming Sylow I and II we prove the following:

Thm (pq^m - Thm)
Let G be a finite group, $|G| = pq^m$, where p, q are prime, $q^m < p$.
Then $G \cong C_p \rtimes_h Q$ where Q is a group $|Q| = q^m$ and $h: Q \mapsto Aut(C_p)$ is some homomorphism.

Proof
The above Sylow counting argument shows G has a unique subgroup of order p.
K is necessarily normal.
To see this let $g \in G$.
Consider the automorphism $\alpha_g : G \mapsto G$,
$\alpha_g(h) = ghg^{-1}$ (congugation).
So $\alpha_g(h)$ is also a subgroup of G, α_g is bijective
so $|\alpha_g(K)| = |K| = p$.
By uniqueness $\alpha_g(K) = K$
i.e. $\forall g \in G \quad gKg^{-1} = K$ or $gK = Kg$
and $K \lhd G$.
$|G| = pq^m$. (q prime, $p \neq q$)
Sylow I tells us that G also has a subgroup Q with $|Q| = q^m$.
Observe that $|G| = |K||Q| = pq^m$
$K \cap Q = \{1\}$ by Lagrange.
Observe if $z \in K \cap Q$, $z \neq 1$.
$ord(z) = p$ ($p \in K$)
$ord(z)$ divides q^m (Lagrange)
$\times$ contradiction.
By Recognition Criterion, $G \cong K \rtimes_h Q$
So $G \cong C_p \rtimes_h Q$

$\square$

MATH 7202

03-02-17

In the above, we don't know what Q looks like.
It can be any group of order q^m.

More general form of Sylow Counting argument is...
Suppose $|G| = pC$
where p is prime and C coprime to p, $C < p$.
Then G has a normal subgroup K of order p.

<u>Proof</u>
Sylow I says that G has at least one subgroup
K, $|K| = p$, so $K \cong C_p$.
Let N_p be the number of such groups.
Sylow II says that $N_p \equiv 1 \mod p$.
So either $N_p = 1$
or $N_p \geq p+1$.
Suppose $N_p \geq p+1$.
Let $K = K_1, K_2, \dots, K_{p+1}$ be distinct subgroups of order p.
If $i \neq j$ then $K_i \cap K_j = \{1\}$
(argument as above).
Each K_i has $(p-1)$ elements of order p.
So get at least $(p+1)(p-1) = p^2 - 1$ elements of order p.
Include Id (ord $1 = 1$) so G has at least p^2 elements.

$$p^2 \leq |G| \leq pC < p^2 \quad (C < p)$$

※ contradiction.

So G has a unique subgroup K, $|K| = p$, $K \cong C_p$.
K is necessarily normal.
If $g \in G$, $|gKg^{-1}| = |K| = p$
So $gKg^{-1} = K$, $gK = Kg$.
$\square$

Think!

$|G| = 12 = 3 \times 2^2$

(snag: $3 < 2^2$)

Use Sylow counting to show that either

1). G has a normal subgroups of order 3

or 2). " " " " " " " 4.

MATH 7202

07-02-17

Group actions

G is a group, X is a set.

By a left action of G on X we mean a mapping

$\bullet : G \times X \mapsto X$, $\bullet(g,x) = g \bullet x$

satisfying

i). $g \bullet (h \bullet x) = (g \bullet h) \bullet x \quad \forall g,h \in G, \forall x \in X.$

ii). $1 \cdot x = x \quad \forall x \in X$

Likewise by a right action: $\bullet : X \times G \mapsto X$,

$\bullet(x,g) = x \cdot g$ satisfying

i). $(x \circ h) \circ g = x \cdot (h \cdot g) \quad \forall x \in X, \forall g,h \in G$

ii). $x \cdot 1 = x \quad \forall x \in X.$

We can reformulate this as follows:

X is a set

$\sigma_X = \{ f : X \mapsto X \mid f \text{ bijective} \}$

Prop

σ_X is a group w.r.t. composition.

$1 = Id_X$, f bijective $\Rightarrow f^{-1}$ bijective

σ_X = group of permutations on X.

from MATH 1201, $X = \{1, 2, \dots, n\}$, $\sigma_X = \sigma_n$ (permutations on n objects) $|\sigma_n| = n!$

Suppose we have a homomorphism

$\psi : G \mapsto \sigma_X$

then we get a left action as follows

$\bullet : G \times X \mapsto X$, $g \bullet x = \psi(g)(x)$

We can check this satisfies the axioms.

Conversely if $\cdot\ G \times X \mapsto X$ is a left action
define $\psi : G \mapsto \sigma_X$ by $\psi(g)(x) = g \cdot x$.
We can check this is a homomorphism.

Example

$G = D_6 = \{1, x, x^2, y, xy, x^2y\}$, $x^3 = y^2 = 1$, $yx = x^2y$

	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

$$x^2 = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$
$$x^2 = \begin{pmatrix} 1 & x & x^2 & y & xy & x^2y \\ x^2 & 1 & x & x^2y & y & xy \end{pmatrix}$$
$$\begin{array}{cccccc} 3 & 1 & 2 & 6 & 4 & 5 \end{array}$$

$$\Rightarrow x^2 \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix}$$

Cayley's Theorem

Let G be a group.
Put $\sigma_G = \{f : G \mapsto G \mid f \text{ is a bijective mapping}\}$
The mapping $\lambda : G \mapsto \sigma_G$, $\lambda(g)(x) = gx$ is such that
λ is an injective homomorphism.

Proof

Let $g, h \in G$, $x \in G$.

$$\begin{aligned} \lambda(gh)(x) = (gh)x &= g(hx) \\ &= \lambda(g)(hx) = \lambda(g)[\lambda(h)(x)] \\ &= [\lambda(g) \circ \lambda(h)](x) \end{aligned}$$

which is true for all x, $\lambda(gh) = \lambda(g) \circ \lambda(h)$
so λ is a homomorphism.

MATH 7202

07-02-17

λ is also injective.
$\lambda(g) = \lambda(h)$ then evaluating on $1 \in G$:
$\lambda(g)(1) = \lambda(h)(1)$
$\Rightarrow g \cdot 1 = h \cdot 1 \Rightarrow g = h$
so $\lambda(g) = \lambda(h) \Rightarrow g = h$

$\square$

Cayley's Theorem
In practical terms....
If G is a group then G is isomorphic to a subgroup of σ_G.

Proof
$\lambda : G \mapsto \sigma_G$
$\lambda : G \overset{\sim}{\Rightarrow} Im(\lambda)$ is an isomorphism

$\square$

D_6 imbeds as a subgroup of σ_6
$|D_6| = 6$, $|\sigma_6| = 6! = 720$.

$1 \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$ $x \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}$

$x^2 \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix}$ $y \sim \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$

The groups σ_n contain all possible finite groups as subgroups.
$\circ : X \times G \mapsto X \Leftrightarrow \lambda : G \mapsto \sigma_G$
$\rho : G \mapsto \sigma_G$, $\rho(g)(x) = x g^{-1}$
ρ is a homomorphism.
$\rho(gh)(x) = x(gh)^{-1} = x h^{-1} g^{-1} = \rho(g)(x h^{-1})$
$= \rho(g)\rho(h)(x)$

A Latin square is a combinatorial device in which every row gives a distinct permutation and " column " " " ".
Groups give Latin squares, converse is false.

Conjugation

If we combine the left and right actions

$c : G \mapsto Aut(G) \ (\subset \sigma_G)$

$c(g)(x) = gxg^{-1}$

In fact $c(g) \in Aut(G)$

Prop

$c : G \mapsto Aut(G)$ is a homomorphism.

Def

Let $\circ : G \times X \mapsto X$ be a left action.

Let $x \in X$.

Define $\langle x \rangle = \{g \cdot x : g \in G\}$.

$\langle x \rangle$ is the orbit of x.

Prop

Let $\circ : G \times X \mapsto X$ be a left action.

Let $x, y \in X$ then

either (i) $\langle x \rangle = \langle y \rangle$

or (ii) $\langle x \rangle \cap \langle y \rangle = \emptyset$

Proof

Suppose $z \in \langle x \rangle \cap \langle y \rangle$

Can write $z = g \cdot x$, $z = h \cdot y$ for some $g, h \in G$

Let $y' \in \langle y \rangle$, $y' = \gamma \cdot y$

$g \cdot x = h \cdot y \Rightarrow y = (h^{-1}g) \cdot x$

so $y' = \gamma . (h^{-1}g) \cdot x$ so $y' \in \langle x \rangle$

so $\langle y \rangle \subset \langle x \rangle$. Similarly $\langle x \rangle \subset \langle y \rangle$

So $\langle x \rangle \cap \langle y \rangle \neq \emptyset \Rightarrow \langle x \rangle = \langle y \rangle$ $\square$

MATH 7202

07-02-17

Example

Consider $G = D_6$ acting on $X = D_6$ by conjugation.

$g \cdot z = gzg^{-1}$

Take $z \in D_6$ in turn.

$z=1$: $g \cdot 1 = g1g^{-1} = 1$, $\langle 1 \rangle = \{1\}$

$z=x$: $y \cdot x = yxy^{-1} = x^2$, $\langle x \rangle = \{x, x^2\}$

$z=x^2$: $y \cdot x^2 = yx^2y^{-1} = x$

$x^a x x^{-a} = x$, $x^a yx (x^a y)^{-1} = x^a x^2 x^{-a}$

$\underset{\underset{1y1^{-1}}{\shortparallel}}{1 \cdot y} = 1$

$xyx^{-1} = xyx^2 = xxy$

$x^2yx^{-2} = x^2yx = x^2x^2y = x$

$\langle y \rangle = \{y, xy, x^2y\}$ Class eqn.

$D_6 = \langle 1 \rangle \amalg \langle x \rangle \amalg \langle y \rangle$. $\leftarrow$ Three orbits

MATH 7202

10-02-17

$G = D_{10} = \{1, x, x^2, x^3, x^4, y, xy, x^2y, x^3y, x^4y\}$

$x^5 = 1, \quad y^2 = 1, \quad yx = x^4y$

Take $X = D_{10}$ and take action to be conjugation $G \times X \mapsto X$

$g \cdot z = gzg^{-1}$

For each $z \in X$ $(= D_{10})$ consider the orbit

$\langle z \rangle = \{g \cdot z (= gzg^{-1}) \mid g \in \underbrace{D_{10}}_{G}\}$

$\langle 1 \rangle = \{1\} \quad g \cdot 1 = g1g^{-1} = 1$

$\langle x \rangle = \{x, x^4\} \quad 1 \cdot x \cdot 1^{-1} = x, \quad x \cdot x \cdot x^{-1} = x,$

$x^2 x x^{-2} = x, \quad x^3 x x^{-3} = x, \quad x^4 x x^{-4} = x,$

$y \cdot x = yxy^{-1} = x^4$

$(xy) \cdot x = xyx(xy)^{-1} = xyxxy = xx^3y^2 = x^4$

$(x^2y) \cdot x = x^2yxx^2y = x^2yx^3y = x^2x^2y^2 = x^4$

$(x^3y) \cdot x = x^3yxx^3y = x^3yx^4y = x^3xy^2 = x^4$

$(x^4y) \cdot x = x^4yxx^4y = x^4yx^5y = x^4$

$\langle x^2 \rangle = \{x^2, x^3\}$

$y \cdot x^2 = yx^2y^{-1} = x^3$

$(xy) \cdot x^2 = x^3 \quad \ldots\ldots$

$\langle y \rangle = \{y, xy, x^2y, x^3y, x^4y\}$

$1 \cdot y \cdot 1^{-1} = y$

$x \cdot y = xyx^{-1} = xyx^4 = x^2y$

$x^2 \cdot y = x^2yx^{-2} = x^2yx^3 = x^4y$

$x^3 \cdot y = x^3yx^{-3} = x^3yx^2 = x^6y = xy$

$x^4 \cdot y = x^4yx^{-4} = x^4yx = x^8y = x^3y$

So $\underset{D_{10}}{\underset{\shortparallel}{G}} \times \underset{D_{10}}{\underset{\shortparallel}{X}} \longmapsto \underset{D_{10}}{\underset{\shortparallel}{X}}, \quad g \cdot z = gzg^{-1}$

Orbits are:

$\langle 1 \rangle = \{1\}$

$\langle x \rangle = \{x, x^4\} \quad (= \langle x^4 \rangle)$

$\langle x^2 \rangle = \{x, x^3\} \; (= \langle x^3 \rangle)$

$\langle y \rangle = \{y, xy, x^2y, x^3y, x^4y\} \; (= \langle x^2y \rangle, \ldots \text{ etc})$

We can denote X as a disjoint union of orbits:

$X = \langle 1 \rangle \sqcup \langle x \rangle \sqcup \langle x^2 \rangle \sqcup \langle y \rangle \quad \leftarrow$ Set theoretic class eqn.

($1, x, x^2, y$ are called orbit representatives)

This is not unique! Could also take $X = \langle 1 \rangle \sqcup \langle x^4 \rangle \sqcup \langle x^3 \rangle \sqcup \langle xy \rangle$

A primitive numerical version of the class eqn. (in this case) is $|X| = |\langle 1 \rangle| + |\langle x \rangle| + |\langle x^2 \rangle| + |\langle y \rangle|$

$$\overset{\shortparallel}{10} = 1 + 2 + 2 + 5$$

To summerise:

G finite group acting on a finite set X

$\cdot : G \times X \mapsto X$,

(i) We can write $X = \langle x_1 \rangle \sqcup \langle x_2 \rangle \sqcup \ldots \sqcup \langle x_m \rangle$

(set theoretic class equation) where $x_1, \ldots, x_m$ represent distinct orbits i.e. $\langle x_i \rangle \cap \langle x_j \rangle = \emptyset \quad (i \neq j)$

(ii) The primitive numerical class equation is $|X| = \sum_{i=1}^{m} |\langle x_i \rangle|$ where $x_1, \ldots, x_m$ represent distinct orbits.

$\cdot : G \times X \mapsto X$, G is a finite group, X is a finite set.

Let $x \in X$, $\langle x \rangle = \{gx : g \in G\}$

Define $G_x = \{g \in G : gx = x\}$

Prop G_x is a subgroup of G

Prop $1 \in G_x$, $1.x = x$.

MATH 7202

10-02-17

If $g, h \in G_x$, $(gh)\cdot x = g\cdot(h\cdot x) = g\cdot x = x$
so $gh \in G_x$ (closed w.r.t. product)
If $g \in G_x$, $g\cdot x = x$
$$g^{-1}(g\cdot x) = g^{-1}\cdot x$$
$$\Rightarrow g^{-1}gx = g^{-1}x \Rightarrow x = g^{-1}x$$
$\Rightarrow g^{-1} \in G_x$ (closed w.r.t. inverses)

Prop
There is a (natural) bijection
$$\nu : G/G_x \xrightarrow{\simeq} \langle x \rangle \quad | \ \forall x \in X$$

Proof
Recall that elements of G/G_x are cosets $\gamma\cdot G_x$ $(\gamma \in G)$
The same cosets can be represented (in general) in different ways.
If $\gamma, \delta \in G$ then $\gamma G_x = \delta G_x$
$\iff \delta^{-1}\gamma \in G_x$ (Rule of Equality)
Define $\nu : G/G_x \longrightarrow \langle x \rangle$
$\nu(\gamma\cdot G_x) = \gamma\cdot x$ $(\in \langle x \rangle)$
The only question is whether this is well defined.

WTS: If $\gamma\cdot G_x = \delta\cdot G_x$ then $\nu(\gamma\cdot G_x) = \nu(\delta\cdot G_x)$.

If $\gamma\cdot G_x = \delta\cdot G_x$ then $\delta^{-1}\gamma \in G_x$
so $(\delta^{-1}\gamma)\cdot x = x$ as $\delta^{-1}\gamma \in G_x$
$\gamma\cdot x = \delta\delta^{-1}(\gamma\cdot x) = \delta\cdot x$.
So ν is well defined.

Claim that ν is a bijection.
ν surjective: If $\gamma\cdot x \in \langle x \rangle$ then $\nu(\gamma\cdot G_x) = \gamma\cdot x$
so ν surjective ✓

ν injective: Suppose $\nu(\gamma \cdot G_x) = \nu(\delta \cdot G_x)$

$\Rightarrow \gamma \cdot G_x = \delta \cdot G_x$

so $(\delta^{-1}\gamma) \cdot x = x$

so $\delta^{-1}\gamma \in G_x$ and $\gamma \cdot G_x = \delta \cdot G_x$ so ν injective ✓

$\square$

$G/G_x \longleftrightarrow \langle x \rangle$

so $\dfrac{|G|}{|G_x|} = |\langle x \rangle|$ True for all $x \in X$.

Return to primitive numerical class equation

$$|X| = \sum_{i=1}^{m} |\langle x_i \rangle| \quad , \quad x_1, \ldots, x_m \text{ are orbit reps.}$$

By above $|\langle x_i \rangle| = |G| / |G_{x_i}|$

To aviod double suffix write $G_i = G_{x_i}$

$$|X| = \sum_{i=1}^{m} |G| / |G_i| \quad , \quad x_1, \ldots, x_m \text{ represent distinct orbits.}$$

↑ Sophisticated Class Equation (Orbit-Stabiliser Eq^n).

Note that $|\langle x \rangle|$ divides $|G|$

$|\langle x \rangle| = |G| / |G_x|$

Go back to D_{10} acting on itself by conjugation.

$$D_{10} = \langle 1 \rangle \sqcup \underset{\{x, x^4\}}{\langle x \rangle} \sqcup \underset{\{x^2, x^3\}}{\langle x^2 \rangle} \sqcup \underset{\{y, xy, x^2y, x^3y, x^4y\}}{\langle y \rangle}$$

$G_1 = \{ g \in D_{10} : g \cdot 1 \cdot g^{-1} = 1 \} = D_{10}$

$G_x = \{ g \in D_{10} : g x g^{-1} = x \}$

MATH 7202

10-02-17

$1 \in G_x$, $x \in G_x$ as $xxx^{-1} = x$
infact $x^a \in G_x$ as $x^a x x^{-a} = x$

So $G_x = \{1, x, x^2, x^3, x^4\}$

y, xy, x^2y, x^3y, x^4y are not in G_x

$|G_x| = 5$, $|\langle x \rangle| = 2 = 10/5$

$G_{x^2} = \{1, x, x^2, x^3, x^4\}$
$G_y = \{1, y\}$

$10 = 1 + 2 + 2 + 5$ ⟵ primitive
$10 = \frac{10}{10} + \frac{10}{5} + \frac{10}{5} + \frac{10}{2}$ ⟵ sophisticated.

Fixed point set
$\cdot : G \times X \mapsto X$ Fixed point set.
$X^G = \{x \in X : \forall g \in G, g \cdot x = x\}$
i.e. $X^G = \{x \in X : G_x = G\}$

Another way of saying this is that
X^G consists of the $x \in X$ such that
$\langle x \rangle = \{x\}$ i.e. $|\langle x \rangle| = 1$

Under an action $\cdot : G \times X \mapsto X$ (G, X finite)
if we list the orbit representatives
$x_1, \dots, x_m$ such that
$X^G = \{x_1, \dots, x_k\}$, $k = |X^G|$
and where $x_i \notin X^G$ for $k+1 \leq i$
If we do this then
$|X| = \sum_{i=1}^{m} |G|/|G_x|$ becomes the following:

Prop

$$|X| = |X^G| + \sum_{i=k+1}^{m} |G| / |G_{x_i}|$$

where $|G_{x_i}| < |G|$ for $k+1 \leq i \leq m$

Proof

$x \in X^G \iff G_x = G$

so $x \notin X^G \iff G_x \subsetneq G$

$x \notin X^G \iff |G_x| < |G|$

$\square$

Example

$\underset{D^{10}}{G} \times \underset{D^{10}}{X} \longmapsto \underset{D^{10}}{X}$, $g.x = gxg^{-1}$

$$|X| = \underset{\{1\}}{\langle 1 \rangle} \sqcup \underset{\{x, x^4\}}{\langle x \rangle} \sqcup \underset{\{x^2, x^3\}}{\langle x^2 \rangle} \sqcup \underset{\{y, xy, x^2y, x^3y, x^4y\}}{\langle y \rangle}$$

Only one fixed point, 1, in this case
($gzg^{-1} = z \iff z = 1 \ \forall g \in G$)

$X^G = \{1\} = \langle 1 \rangle$

$$|X| = 1 + \sum_{i=2}^{4} |G| / |G_i|$$

$$= 1 + \frac{10}{5} + \frac{10}{5} + \frac{10}{2}$$

$G_x = \{1, x, x^2, x^3, x^4\}$, $G_x \neq G$

$G_{x^2} = \{1, x, \dots, x^4\}$, $G_{x^2} \neq G$

$G_y = \{1, y\}$, $G_y \neq G$.

MATH 7202

10-02-17

Special case

Suppose $G = P$ is a group with $|P| = p^n$, p prime and consider action of P on a finite set X.

$P \times X \mapsto X$

Theorem

Let P be a group of order p^n acting on a finite set X: $\bullet : P \times X \longmapsto X$ (p prime)

Then $|X^P| \equiv |X| \pmod p$

Proof

Write Class eq^n in above form.

$$|X| = |X^P| + \sum_{i=k+1}^{m} |P|/|P_{x_i}| \quad \text{and} \quad |P_{x_i}| < |P|$$

$(k = |X^P|)$

$|P| = p^n$, p prime so

$|P_{x_i}| = p^{e_i}$, $e_i < n$

$$|X| = |X^P| + \sum_{i=k+1}^{m} p^{(n-e_i)}$$

and $0 < n - e_i$ as $e_i < n$.

Calculate mod p, $p^{n-e_i} \equiv 0 \pmod p$

so $|X| \equiv |X^P| \bmod p$.

$\square$

This is a very special case of the Class Eqn, only when $|G| = |P| = p^n$, p prime.

Wilson's Theorem

Let p be a prime, k a positive integer

$\binom{kp^n}{p^n} \equiv k \mod p$ ← binomial coefficient.

Proof

Let G be some group with $|G| = p^n$

(example: could take $G = C_{p^n}$)

Take $X = G \times \{1, \dots, k\}$

Then $|X| = |G| \times k = kp^n$

Let G act on X as follows

$* : G \times X \mapsto X \quad , \quad g * (h, i) = (gh, i)$

Def

$\mathcal{X} = \{A : A \subset X \text{ and } |A| = p^n\}$

$|X| = kp^n$

$|\mathcal{X}| = \binom{kp^n}{p^n}$

Define an action of G on $\mathcal{X}$ as follows.

If $A \subset X$ define $g \cdot A = \{g * a : g \in G\}$

Clearly $|g \cdot A| = |A|$

$G \times \mathcal{X} \mapsto \mathcal{X}$

$g \cdot A = \{g \cdot a : a \in A\}$

Since $|G| = p^n$ then $|\mathcal{X}| \equiv |\mathcal{X}^G| \pmod p$

Need only to calculate $\mathcal{X}^G$.

Observe that each set $G \times \{i\} \in \mathcal{X}^{(*)}$

and $G \times \{i\} \in \mathcal{X}^G$

$g \cdot (h, i) = (gh, i)$,

$g \cdot (G \times \{i\}) = G \times \{i\}$

MATH 7202

10-02-17

Claim that every fixed point is of this form (*).
Take $A \subset \mathcal{X}$, $|A| = p^n$.
Let $\alpha \in A$ so α looks like $\alpha = (h, i)$, $h \in G$.

If $g \cdot A = A$ clearly $g \cdot \alpha \in A$ $\forall g \in G$,
$(gh, i) \in A$ $\forall g \in G$.

We get a mapping $\mu : G \mapsto A$ $\mu(g)(h,i) = (gh, i)$

μ injective:

$\mu(g_1) = \mu(g_2)$

$\mu(g_1)(h,i) = \mu(g_2)(h,i)$

$(g_1 h, i) = (g_2 h, i)$

$g_1 h = g_2 h \Rightarrow g_1 = g_2$ ✓

$|A| = |G|$ so $A = Im(\mu) = \{(\gamma, i) : \gamma \in G\}$
Essential point is that 2nd coordinate, i, can't change within a fixed point.
i.e. every fixed point has the form
$G \times \{i\}$ $(1 \leq i \leq k)$ so $|\mathcal{X}^G| = k$.

i.e. $|\mathcal{X}| \equiv |\mathcal{X}^G|$ (mod p)
means that $\binom{kp^n}{p^n} \equiv k$ (mod p)

$\square$

MATH 7202

21-02-17

Theorem (Sylow I)

p prime, $k \in \mathbb{Z}$ with k coprime to p.
G is a finite group with $|G| = kp^n$.
Then G has a subgroup of order p^n

Proof (By induction on k)
For $k=1$ there is nothing to prove.
Assume true for integers $k' < k$ and suppose that $|G| = kp^n$ (so $1 < k$).
Let $\mathcal{A} = \{A \mid A \subset G, |A| = p^n\}$ (Here A is just a subset).
Then $|\mathcal{A}| = \binom{kp^n}{p^n}$

If $g \in G$, $A \in \mathcal{A}$ then
define $g \cdot A = \{ga : a \in A\}$

This gives a left action
$G \times \mathcal{A} \mapsto \mathcal{A}$, $g \cdot A = \{ga \mid a \in A\}$
Note that for this action, there are no fixed points!
Why? Suppose A is fixed under the action. Choose $a \in A$
Then there is a mapping $i : G \mapsto A$, $i(g) = g \cdot a$

? This is well defined if A is a fixed point.
i is necessarily injective.

$i(g_1) = i(g_2)$

$\Rightarrow g_1 a = g_2 a$

$\Rightarrow g_1 a a^{-1} = g_2 a a^{-1} \Rightarrow g_1 = g_2$

But $|G| = kp^n > |A| = p^n$ *contradiction.
Consider the Class Eq^n.
Let $A_1, \dots, A_m$ be orbit representatives.
Let $G_i = G_{A_i}$ (stability group of A_i)
Because there are no fixed points,

$|G_i| < |G|$.

We can write $|G_i| = k_i p^{e_i}$

where $\begin{cases} k_i \text{ is coprime to } p, \\ e_i \leq n, \\ k_i p^{e_i} < k p^n. \end{cases}$

Class Eq^n looks like

$$|A| = \sum_{i=1}^{m} |G| / |G_i|$$

$$\Rightarrow |A| = \sum_{i=1}^{m} \left(\frac{k}{k_i}\right) p^{n-e_i}$$

By Wilson's Thm,

$|A| \equiv k \pmod{p}$

so LHS $\not\equiv 0 \pmod{p}$

If each $e_i < n$,

$p^{n-e_i} \equiv 0 \pmod{p}$

so then RHS $\equiv 0 \pmod{p}$.

So for at least one i, $e_i = n$

and $|G_i| = k_i p^n < k p^n$

so $k_i < k$

By induction, G_i has a subgroup, H,

$|H| = p^n$.

But G_i is a subgroup of G so H is a subgroup

G and $|H| = p^n$.

This completes induction

$\square$

Before we can prove Sylow II,

we need to consider Quotient Groups.

MATH 7202

21-02-17

Quotient Groups

Let G be a group and $K \triangleleft G$ a normal subgroup. We show how to make G/K into a group. $G/K = \{gK \mid g \in G\}$

Rule of Equality

$$g_1 K = g_2 K \iff g_2^{-1} g_1 \in K \quad [K \triangleleft G]$$

Define $\cdot : G/K \times G/K \longrightarrow G/K$ such that

$$(gK)\cdot(hK) = ghK$$

Prop

This is well defined provided $K \triangleleft G$.

Proof

Must show that if $g_1 K = g_2 K$ and $h_1 K = h_2 K$ then $(g_1 h_1)K = (g_2 h_2)K$

ie. got to show that $(g_2 h_2)^{-1} g_1 h_1 \in K \Leftrightarrow h_2^{-1}(g_2^{-1} g_1) h_1 \in K$

Since $g_1 K = g_2 K$ then $g_2^{-1} g_1 \in K$.

But $K \triangleleft G$ so for any $\gamma \in G$, $\gamma(g_2^{-1} g_1)\gamma^{-1} \in K$

Take $\gamma = h_2^{-1}$, $\gamma^{-1} = h_2$

so $h_2^{-1}(g_2^{-1} g_1) h_2 \in K$

But $h_2^{-1} h_1 \in K$ because $h_1 K = h_2 K$

so $h_2^{-1}(g_2^{-1} g_1) h_2 h_2^{-1} h_1 \in K$

ie. $h_2^{-1} g_2^{-1} g_1 h_1 \in K$ so $(g_2 h_2)^{-1} g_1 h_1 \in K$

ie. $g_1 h_1 K = g_2 h_2 K$ as required.

$\square$

So if $K \triangleleft G$ we now have a well defined map: multiplication:

$$\cdot : G/K \times G/K \mapsto G/K \quad , \quad (gK)\cdot(hK) = ghK.$$

Let's check group axioms for G/K.

<u>Associativity</u>

$$(gK)\cdot[(hK)\cdot(nK)] = [(gK)\cdot(hK)]\cdot(nK)$$

<u>Why?</u>

$$\begin{aligned}(gK)\cdot[(hK)\cdot(nK)] &= (gK)\cdot(hnK) \\ &= g\cdot(hn)K \qquad g\cdot(hn)=(gh)\cdot n \text{ in } G \\ &= (gh)\cdot nK \\ &= (ghK)\cdot(nK) \\ &= [(gK)\cdot(hK)]\cdot(nK) \checkmark\end{aligned}$$

<u>Identity</u>

Try $1\cdot K$

$(gK)\cdot(1\cdot K) = (g\cdot 1)K = gK$

$(1\cdot K)\cdot(gK) = (1\cdot g)K = gK$

So $1\cdot K$ is the identity. ✓

Note that $1\cdot K = K = \{1\cdot k : k\in K\} = \{k\in K\}$

So K is the identity in G/K

<u>Inverses</u>

$(gK)\cdot(g^{-1}K) = (gg^{-1})K = 1\cdot K = K$

$(g^{-1}K)\cdot(gK) = (g^{-1}g)K = 1\cdot K = K$

So inverses exist. ✓

We've proved:

<u>Prop</u>

If $K \lhd G$ then G/K is a group.

Observe we have a mapping

$\varphi: G \mapsto G/K$, $\varphi(g) = gK$ (Identification map)

MATH 7202

21-02-17

Prop

ψ is a homomorphism.

Proof

(Tautologous)

$$\psi(gh) = (gh)K$$
$$= (gK)\cdot(hK)$$
$$= \psi(g)\psi(h)$$

$\square$

Question:

G finite, $K \triangleleft G$, $|G/K| = \dfrac{|G|}{|K|}$

Example

$G = Q(8) = \{1, -1, i, -i, j, -j, k, -k\}$

Take $K = \{1, -1\}$, $K \triangleleft G$

$|K| = 2$, $|G| = 8$

So $|G/K| = 8/2 = 4$

There are two groups of order 4 : C_4, $C_2 \times C_2$

Which group is $Q(8)/\{\pm 1\}$?

Calculate!

$(iK)\cdot(iK) = i^2 K$, $i^2 = -1 \in K$

so $(iK)\cdot(iK) = K$

Similarly $(jK)(jK) = (-1)K = K$

and $(kK)(kK) = (-1)K = K$

Every element γ of $Q(8)/\{\pm 1\}$ satisfies $\gamma^2 = 1$

So $Q(8)/\{\pm 1\} \cong C_2 \times C_2$

MATH 7202

24-02-17

E. Noether Isomorphisms

Let $\varphi : G \mapsto H$

be a group homomorphism.

$Ker(\varphi) := \{g \in G : \varphi(g) = 1\}$ $\varphi(g)=1$ as this is multiplicative

$Im(\varphi) := \{h \in H : \exists g \in G, \varphi(g) = h\}$

$T : V \mapsto W$ additive

$Ker(T) = \{v \in V : T(v) = 0\}$

Prop

$Ker(\varphi)$ is a normal subgroup of G

Proof

$1 \in Ker(\varphi)$, $\varphi(1) = 1$ Identity ✓

Suppose $g_1, g_2 \in Ker(\varphi)$

$\varphi(g_1) = 1$, $\varphi(g_2) = 1$

$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 1 \cdot 1 = 1$

$\Rightarrow g_1 g_2 \in Ker(\varphi)$ Closure w.r.t. product ✓

Suppose $g \in Ker(\varphi)$

$gg^{-1} = 1$ so

$\varphi(gg^{-1}) = 1$ so $\varphi(g)\varphi(g^{-1}) = 1$

But $\varphi(g) = 1 \Rightarrow \varphi(g^{-1}) = 1$

$\Rightarrow g^{-1} \in Ker(\varphi)$ Closure w.r.t. inverses ✓

So $Ker(\varphi)$ is a subgroup of G.

Claim that $Ker(\varphi) \triangleleft G$

Let $x \in Ker(\varphi)$, $\varphi(x) = 1$, let $\gamma \in G$

Got to show $\gamma x \gamma^{-1} \in Ker(\varphi)$

$$\begin{aligned}\varphi(\gamma x \gamma^{-1}) &= \varphi(\gamma)\varphi(x)\varphi(\gamma^{-1}) \\ &= \varphi(\gamma) \cdot 1 \cdot \varphi(\gamma^{-1}) \\ &= \varphi(\gamma\gamma^{-1}) = \varphi(1) = 1\end{aligned}$$

So $\gamma x \gamma^{-1} \in Ker(\varphi)$

$\square$

Prop

$\mathrm{Im}(\varphi)$ is a subgroup of H.

(Beware: it is not usually normal).

Proof

$1_H \in \mathrm{Im}(\varphi)$, $\varphi(1_G) = 1_H$ Identity ✓

Suppose $h_1, h_2 \in \mathrm{Im}(\varphi)$

Choose $g_1, g_2 \in G$ ...

$\varphi(g_1) = h_1$, $\varphi(g_2) = h_2$

$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$

So $h_1 h_2 \in \mathrm{Im}(\varphi)$ Closure w.r.t. products ✓

Suppose $h \in \mathrm{Im}(\varphi)$

Got to show $h^{-1} \in \mathrm{Im}(\varphi)$

Choose $g \in G : \varphi(g) = h$

Consider:

$1 = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) = h\varphi(g^{-1})$

$1 = \varphi(g^{-1}g) = \varphi(g^{-1})\varphi(g) = \varphi(g^{-1})h$

So $\varphi(g^{-1}) = h^{-1}$

and $h^{-1} \in \mathrm{Im}(\varphi)$ Closure w.r.t. inverses ✓

$\square$

Noether's Basic Isomorphism Thm

Let $\varphi : G \mapsto H$ be a group homomorphism,

then $\dfrac{G}{\mathrm{Ker}(\varphi)} \cong \mathrm{Im}(\varphi)$

Proof

Put $K = \mathrm{Ker}(\varphi)$.

$K \triangleleft G$ so I have a quotient group G/K.

Going to show $G/K \cong \mathrm{Im}(\varphi)$.

Define $\varphi_* : G/K \longrightarrow \mathrm{Im}(\varphi)$

by $\varphi_*(gK) = \varphi(g)$.

MATH 7202

24-02-17

Need to show this is well defined.

i.e. Suppose $g_1 K = g_2 K$.

Got to show $\varphi_*(g_1 K) = \varphi_*(g_2 K)$

i.e. $\varphi(g_1) = \varphi(g_2)$

Rule of equality: $g_1 K = g_2 K \Rightarrow g_2^{-1} g_1 \in K = \mathrm{Ker}(\varphi)$

Apply φ:

$$\varphi(g_2^{-1} g_1) = 1$$
$$\Rightarrow \varphi(g_2^{-1})\varphi(g_1) = 1$$
$$\Rightarrow \varphi(g_2)^{-1}\varphi(g_1) = 1$$
$$\Rightarrow \varphi(g_1) = \varphi(g_2)$$

So φ_* is well defined.

$\varphi_* : G/K \longmapsto \mathrm{Im}(\varphi)$ is a group homomorphism ← claim.

$$\varphi_*((g_1K)(g_2K)) = \varphi_*(g_1 g_2 K) \quad \left((\gamma K)(\delta K) = \gamma\delta K \text{ as } K \text{ is normal}\right)$$
$$= \varphi(g_1 g_2)$$
$$= \varphi(g_1)\varphi(g_2)$$
$$= \varphi_*(g_1K)\varphi_*(g_2K)$$

So $\varphi_*((g_1K)(g_2K)) = \varphi_*(g_1K)\varphi_*(g_2K)$ homomorphism ✓

φ_* is obviously surjective ✓

If $h \in \mathrm{Im}(\varphi)$, $h = \varphi(g)$

so $h = \varphi_*(gK)$

Remains to show φ_* is injective.

Suppose

$$\varphi_*(g_1K) = \varphi_*(g_2K)$$

Then $\varphi(g_1) = \varphi(g_2)$

$\varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) = 1$

So $g_2^{-1}g_1 \in K = \mathrm{Ker}(\varphi)$ (Rule of Equality)

So $\varphi_*(g_1K) = \varphi_*(g_2K) \Rightarrow g_1K = g_2K$ Injective ✓

$\square$

Suppose G is a group,
P, Q subgroups.
$PQ = \{pq : p \in P, q \in Q\}$
Is PQ necessarily a subgroup of G?
In general: No!
However PQ is a subgroup provided...

Def
Say that P normalises Q when
$\forall g \in P \; \forall y \in Q, \; gyg^{-1} \in Q$
i.e. $gQg^{-1} = Q$.

Prop
If P, Q are subgroups of G and P normalises Q then
1). PQ is a subgroup of G
2). Q is a normal subgroup of PQ.

Proof
The hypothesis is $gyg^{-1} \in Q$ whenever $g \in P$, $y \in Q$.
Got to show $PQ = \{pq : p \in P, q \in Q\}$ is a subgroup.
$1 \in PQ$ as $1 = \underset{\in P}{1} \cdot \underset{\in Q}{1}$

Identity ✓

Suppose $p_1 q_1 \in PQ$, $p_2 q_2 \in PQ$.
Got to show $p_1 q_1 p_2 q_2 \in PQ$
$p_1 q_1 p_2 q_2 = (p_1 p_2)(p_2^{-1} q_1 p_2) q_2$
Take $y = q_1$, $\gamma = p_2^{-1}$
By the normalisation hypothesis
$\gamma y \gamma^{-1} = p_2^{-1} q_1 p_2 \in Q$
But $q_2 \in Q$ so $p_2^{-1} q_1 p_2 q_2 \in Q$.
$p_1 p_2 \in P$ so $p_1 q_1 p_2 q_2 = \underset{\in P}{(p_1 p_2)} \underset{\in Q}{[p_2^{-1} q_1 p_2 q_2]} \in PQ$

closed w.r.t. products ✓

MATH 7202

24-02-17

Let $pq \in PQ$,
got to show $(pq)^{-1} \in PQ$, but $(pq)^{-1} = q^{-1}p^{-1}$
But $q^{-1}p^{-1} = p^{-1}(pq^{-1}p^{-1})$
and $p^{-1} \in P$, $pq^{-1}p^{-1} \in Q$
So $q^{-1}p^{-1} = (pq)^{-1} \in PQ$ closed w.r.t. inverses ✓
So if P normalises Q then PQ is a subgroup of G. Still to show: $Q \triangleleft PQ$.

Observe that $P \subset PQ$ $[p = p \cdot 1,\ 1 \in Q]$
$Q \subset PQ$ $[q = 1 \cdot q,\ 1 \in P]$
Suppose $q \in Q$ and $\gamma \in PQ$.
Got to show $\gamma q \gamma^{-1} \in Q$.
Write $\gamma = p_1 q_1$, $p_1 \in P$, $q_1 \in Q$
$\gamma^{-1} = q_1^{-1} p_1^{-1}$
$\gamma q \gamma^{-1} = p_1 [q_1 q q_1^{-1}] p_1^{-1}$
$q_1 q q_1^{-1} \in Q$, & by Normalisation Condition
$p_1 [q_1 q q_1^{-1}] p_1^{-1} \in Q$
$\square$

__Theorem__ (Noether's 1st Isomorphism Thm)
Let P, Q be subgroups of G and suppose P normalises Q, then
i) Q is a normal subgroup of PQ
ii) $P \cap Q$ is a normal subgroup of P
iii). $PQ/Q \cong P/P \cap Q$

__Proof__
i). Already done
ii). $P \cap Q$ is obviously a subgroup of both P and Q.
$P \cap Q \triangleleft P$. Why?
Let $\gamma \in P \cap Q$, $p \in P$.
$p \gamma p^{-1} \in P$ because $\gamma \in P$.

$p\gamma p^{-1} \in Q$ normalisation condition because $\gamma \in Q$

$\gamma \in P \cap Q$, $p \in P$

$\Rightarrow$ $p\gamma p^{-1} \in P \cap Q$ $\square$

iii). Formal claim is that $PQ/Q \cong P/P\cap Q$

Define $\nu : P \mapsto PQ/Q$

by $\nu(p) = pQ$ $(= (p.1)Q)$

ν is a group homomorphism. Why?

$\nu(p_1 p_2) = (p_1 p_2)Q$

$= (p_1 Q)(p_2 Q)$

$= \nu(p_1)\nu(p_2)$

ν is surjective:

Let $X = PQ/Q$

what does X look like?

$X = (pq)Q$, $p \in P$, $q \in Q$

but $qQ = Q$

so $X = pQ$

So $X = \nu(p)$, ν surjective

So $Im(\nu) = \frac{PQ}{Q}$

But $P/Ker(\nu) \cong Im(\nu) = PQ/Q$

what is $Ker(\nu)$?

ans: $Ker(\nu) = P \cap Q$

$Ker(\nu) = \{p \in P : \nu(p) = \text{Identity in } PQ/Q\}$

But identity in PQ/Q is the coset Q

So $Ker(\nu) = \{p \in P : pQ = Q\}$

i.e. $Ker(\nu) = P \cap Q$

$P/P\cap Q = P/Ker(\nu) \cong Im(\nu) = PQ/Q$ $\square$

MATH 7202

24-02-17

Theorem (Sylow II)

Let p be prime, $k \in \mathbb{Z}$, $k \geq 1$ where k is coprime to p. Let G be a group of order kp^n.

N_p = number of subgroups Q of G with $|Q| = p^n$.

Then $N_p \equiv 1 \pmod{p}$.

Proof

Let $S(p) = \{Q : Q \text{ is a subgroup of } G \text{ and } |Q| = p^n\}$

Sylow I tells us that $S(p) \neq \emptyset$

Choose an element $P \in S(p)$.

So P is a subgroup of G, $|P| = p^n$.

Let P act on $S(p)$ as follows:

$\bullet : P \times S(p) \longmapsto S(p)$

$g \bullet Q = gQg^{-1}$

Clearly gQg^{-1} is a subgroup of G

$|gQg^{-1}| = |Q| = p^n$

$|P| = p^n$ so by the Class Eq^n

$|S(p)| \equiv |S(p)^P| \pmod{p}$

where $S(p)^P$ is the fixed point set

$Q \in S(p)^P \Leftrightarrow gQg^{-1} = Q \quad \forall g \in P$

So $Q \in S(p)^P \Leftrightarrow P$ normalises Q

Now $N_p = |S(p)|$ by definition.

Note that $P \in S(p)^P$ $[p P p^{-1} \in P, \ p_1 p_1 \in P]$

I claim that P is the only fixed point.

To see this suppose that $Q \in S(p)^P$ so P normalises Q.

So $\frac{PQ}{Q} \cong \frac{P}{P \cap Q}$

$$\frac{|PQ|}{|Q|} = \frac{|P|}{|P \cap Q|}$$

So $|PQ| = |Q| \times \left(\frac{|P|}{|P \cap Q|}\right)$

$|Q| = p^n$, $|P| = p^n$

So $\frac{|P|}{|P \cap Q|} = p^e$ where $0 \leq e \leq n$

So $|PQ| = p^{n+e}$ for some e, $0 \leq e \leq n$.

But PQ is a subgroup of G.

$|G| = kp^n$, k coprime to p.

p^{n+e} divides kp^n, k coprime to p.

So $e = 0$ and $|PQ| = p^n$

$P \subset PQ$ and $|P| = p^n$

So $P = PQ$

Also $Q \subset PQ$, $|Q| = p^n$

so $Q = PQ$

So $P = PQ = Q$

$Q \in S(p)^P \to Q = P$

ie. unique fixed point.

$|P| = p^n$ so by Class Eq^n

$|S(p)| \equiv |S(p)^P| \pmod{p}$

So $|S(p)^P| = 1$, $|S(p)| = N_p$

So $N_p \equiv 1 \pmod{p}$

$\square$

Centre of a group

G a group

$Z(G) = \{z \in G : \forall g \in G,\ gz = zg\}$

(The 'centre of G')

Prop

$Z(G) \triangleleft G$

MATH 7202

24-02-17

Proof

$1 \in Z(G)$

$g \cdot 1 = 1 \cdot g \quad \forall g$ Identity ✓

If $z_1, z_2 \in Z(G)$

$\forall g, \quad g(z_1 z_2) = g(z_1) z_2$

$= (z_1 g) z_2$

$= z_1 (g z_2)$

$= (z_1 z_2) g$ Closed under products ✓

Let $z \in Z(G)$

$\forall g \in G, \quad gz = zg$

$z^{-1} g z = z^{-1} z g = g$

$z^{-1} g = g z^{-1}$

so $z^{-1} \in Z(G)$ Closed w.r.t. inverses ✓

So subgroup ✓

$Z(G) \lhd G$?

If $z \in Z(G), \ g \in G$

$g z g^{-1} = z g g^{-1} = z$

$\square$

$Z(D_{4n+2}) = \{1\}$

$Z(D_{4n}) \neq \{1\}$

(can check this)

Prop

If G is a group

$|G| = p^n$, p prime

Then $Z(G) \neq \{1\}$

Proof

Let G act on itself by conjugation

$* : G \times G \mapsto G$

$g * h = ghg^{-1}$

$Z(G)$ is the fixed point set of this action

$|G| = p^n$ so $|G| \equiv |Z(G)| \pmod p$

$|G| \equiv 0 \pmod p$

So $|Z(G)|$ is divisible by p.

so $|Z(G)| > 1$

$\square$

MATH 7202

28-02-17

$\lvert G\rvert$	Possibilities	Complete?	$\lvert G\rvert$	Possibilities	Complete?
1	$\{1\}$	✓	14	C_{14}, D_{14}	✓
2	C_2	✓	15	C_{15}	✓
3	C_3	✓	16	Mess!!	
4	C_4, $C_2 \times C_2$	✓	17	C_{17}	✓
5	C_5	✓	18	five groups	
6	C_6, D_6	✓	19	C_{19}	✓
7	C_7	✓	20		
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, $Q(8)$	✓	21	C_{21}, $G(21) = G(7,3)$	
9	C_9, $C_3 \times C_3$ (coming soon)	✓	22	C_{22}, D_{22}	✓
10	C_{10}, D_{10}	✓	23	C_{23}	✓
11	C_{11}	✓	24	Difficult!!	
12	C_{12}, $C_6 \times C_2$, $D_6 \times C_2$, D_6^*, A_4	✓	25	C_{25}, $C_5 \times C_5$ (coming soon)	✓
13	C_{13}	✓	26	C_{26}, D_{26}	✓

Groups of order 12:

$12 = 2^2 \times 3$

Prop

If $|G| = 12$ then either

(i) G has a normal subgroup of order 3,

or (ii) G has a normal subgroup of order 4.

Proof

Let H be a subgroup, $|H| = 3$.

Let L be a subgroup, $|L| = 4$.

N_3 = no. of subgroups of order 3.

$N_3 \equiv 1 \pmod 3$ so either $N_3 = 1$ or $N_3 \geq 4$.

If $N_3 = 1$ then H is the unique subgroup of order 3 so $H \lhd G$.

If $N_3 \geq 4$, choose 4 distinct subgroups of order 3, H_1, H_2, H_3, H_4 (so $H = H_1$) so G has exactly $4 \times (3-1) = 8$ elements of order 3 (can't have $N_3 = 7$).

However $L \subset G$, $|L| = 4$

$|G| - 8 = 4 = |L|$

So L is a unique subgroup of order 4.

Hence $L \lhd G$.

$\square$

This argument splits groups of order 12 into 4 classes:

I) $K \rtimes_h C_4$ $\quad |K| = 3$

$\Rightarrow C_3 \rtimes_h C_4$

II). $K \rtimes_h (C_2 \times C_2)$ $\quad |K| = 3$

$\Rightarrow C_3 \rtimes_h (C_2 \times C_2)$

III). $C_4 \rtimes_h C_3$ $\quad |K| = 4$

IV). $(C_2 \times C_2) \rtimes_h C_3$ $\quad |K| = 4$

<u>Class I</u>

$C_3 = \{1, x, x^2\}$, $x^3 = 1$

$C_4 = \{1, y, y^2, y^3\}$, $y^4 = 1$

$h: C_4 \mapsto \text{Aut}(C_3) = \{1, \tau\} \cong C_2$

$\tau(x) = x^{-1}$

Two homomorphisms:

0). $h(y) = 1$, 1). $h(y) = \tau$

For 0). $\langle X Y \mid X^3 = 1, Y^4 = 1, YX = XY \rangle$

$\Rightarrow C_3 \times C_4 \cong C_{12}$

For 1). $\langle X Y \mid X^3 = 1, Y^4 = 1, YX = X^2 Y \rangle$

Called either D_6^* or $Q(12)$

<u>Class II</u>

$C_3 = \{1, x, x^2\}$ $x^3 = 1$

$C_2 \times C_2 = \{1, s, t, st\}$ $s^2 = t^2 = 1$, $ts = st$, $(st)^2 = 1$

$h: C_2 \times C_2 \mapsto \text{Aut}(C_3)$

$= \{1, t\} \cong C_2$

MATH 7202

28-02-17

Four homomorphisms:

0). $h(s)=1$, $h(t)=1$, $h(st)=1$

Get $C_3 \times C_2 \times C_2 \cong C_6 \times C_2$

1). $h(s)=\tau$, $h(t)=1$, $h(st)=\tau$

2). $h(s)=1$, $h(t)=\tau$, $h(st)=\tau$

3). $h(s)=\tau$, $h(t)=\tau$, $h(st)=1$

For 1). $\langle X, S, T \mid X^3 = S^2 = T^2 = 1,\ ST = TS,$
$SX = X^2S,\ TX = XT \rangle$

So $G \cong D_6 \times C_2 = \langle X, S \rangle \times \langle T \rangle$

For 2). $G \cong D_6 \times C_2$
$\langle X, T \rangle \times \langle S \rangle$

For 3). $G \cong D_6 \times C_2$
$\langle X, S \rangle \times \langle ST \rangle$

Class III

$C_4 \rtimes_h C_3$

$C_4 = \{1, x, x^2, x^3\}$, $C_3 = \{1, z, z^2\}$

$h: C_3 \mapsto Aut(C_4) \cong C_3$

So h is trivial.

$G \cong C_4 \times C_3 \cong C_{12}$

Class IV

$C_2 \times C_2 = \{1, s, t, st\}$ $s^2 = t^2 = 1$, $st = ts$

$C_3 = \{1, \omega, \omega^2\}$, $\omega^3 = 1$

$h: C_3 \mapsto Aut(C_2 \times C_2) \cong D_6 \cong S_3$

$D_6 = \{1, x, x^2, y, xy, x^2y \mid x^3 = y^2 = 1,\ yx = x^2y\}$

$h: C_3 \mapsto D_6$, three possibilities:

0). $h(\omega) = Id$: $C_2 \times C_2 \times C_3 \cong C_6 \times C_2$

1). $h(\omega) = x$, $x(s) = t$, $x(t) = st$, $x(st) = s$

2). $h(\omega) = x^2$, $x^2(s) = st$, $x^2(t) = s$, $x^2(st) = t$

Either way $G \cong A_4$ ← even permutations on $\{1, 2, 3, 4\}$

MATH 7202

03-03-17

Rings

$\cdot : X \times X \mapsto X$

usual hypotheses on $\cdot$:

i) Associativity : $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

$(X, \cdot)$ is then a Semigroup.

ii). Identity : $1 \cdot x = x = x \cdot 1$

$(X, \cdot, 1)$ is called a Monoid.

iii). Inverses : $\forall x \in X \ \exists y$ s.t. $x \cdot y = 1 = y \cdot x$.

Then $(X, \cdot, 1)$ with inverses is a group.

A ring has two algebraic structures.

By a ring R we mean a 5-tuple $R = (R, +, 0, \cdot, 1)$ where:

i). R is a set, $0, 1 \in R$

ii). $(R, +, 0)$ abelian group (written additively)

iii). $(R, \cdot, 1)$ is a monoid

iv). $\cdot$ distributes over $+$

$$a \cdot (b+c) = a \cdot b + a \cdot c \ , \quad (b+c) \cdot a = b \cdot a + c \cdot a$$

$0 \cdot a = 0 \ \forall a, \ 1 \cdot a = a \ \forall a$

and we insist that $0 \neq 1$.

$[\text{If } 0 = 1 \Rightarrow a = 0 \ \forall a] \leftarrow$ We want to avoid this.

Standard examples

$\mathbb{Z} = (\mathbb{Z}, +, 0, \cdot, 1)$ is a ring

$\mathbb{Z}$ is a commutative ring, i.e. $\forall a, b \in \mathbb{Z} \ a \cdot b = b \cdot a$.

$M_2(\mathbb{Z}) =$ 2x2 matrices over $\mathbb{Z}$ where

$\cdot =$ matrix multiplication, $+ =$ matrix addition, $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

This is a non-commutative ring.

for the most part we'll only consider commutative rings.

Examples

1). $\mathbb{Z}$

2). Any field $\mathbb{F}$ is a commutative ring (not typical)

3). $\mathbb{F}[x]$: ring of polynomials in a single variable x with coefficients in a field $\mathbb{F}$.

A typical element of $\mathbb{F}[x]$ looks like

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \quad , \quad a_i \in \mathbb{F}$$

If $a_n \neq 0$ then $\deg(a(x)) = n$

Rule of Equality

$$a_0 + a_1 x + \dots + a_n x^n = b_0 + b_1 x + \dots + b_n x^n$$
$$\iff a_i = b_i \quad \forall i$$

Addition:

$$a(x) + b(x) = \sum (a_r + b_r) x^r$$

where $a(x) = \sum a_r x^r$, $b(x) = \sum b_r x^r$

Zero: $0(x) = 0 \cdot 1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n$

Identity: $1 = 1 + 0 \cdot x + 0 \cdot x^2 + \dots + 0 \cdot x^n$

Multiplication:

$$a(x) = \sum a_r x^r \quad , \quad b(x) = \sum b_s x^s$$
$$a(x) b(x) = c(x) = \sum c_t x^t$$

where $c_t = \sum_{r+s=t} a_r b_s$

$\mathbb{F}[x]$ behaves very like $\mathbb{Z}$

By comparison, $\mathbb{F}[x_1, x_2, \dots, x_n]$ is the polynomial ring in n variables.

For $n \geq 2$ $\mathbb{F}[x_1, x_2, \dots, x_n]$ is more difficult to study (Algebraic Geometry)

MATH 7202

03-03-17

Ideals and quotient rings

Let $R = (R, +, 0, \cdot, 1)$ be a commutative ring.

By an ideal I in R, I mean

i). I is an additive subgroup of R

ii). $\forall a \in I, \forall \lambda \in R, \lambda \cdot a \in I$

Example

$R = \mathbb{Z}, n \in \mathbb{Z}$

$(n) := \{\mu n : \mu \in \mathbb{Z}\}$

(The set of multiples of n).

Prop

(n) is an ideal

Proof

$0 \in (n)$ as $0 = 0 \cdot n$.

$\mu_1 n \in (n), \mu_2 n \in (n)$

$\Rightarrow \mu_1 n + \mu_2 n = (\mu_1 + \mu_2) n \in (n)$

$-\mu n = (-\mu) n \in (n)$

So (n) is a subgroup.

If $\mu n \in (n), \lambda \in \mathbb{Z}$

then $\lambda \cdot \mu n = (\lambda \mu) n \in (n)$

So (n) is an ideal. $\square$

Def

Let R be a commutative ring, $a \in R$.

Define $(a) = \{\mu a : \mu \in R\}$

Prop

(a) is an ideal in R.

More generally,

if $a_1, \dots, a_m \in R$,

$$(a_1, \dots, a_m) = \left\{ \sum_{i=1}^{m} \mu_i a_i \mid \mu_i \in R \right\}$$

Prop

$(a_1, \dots, a_m)$ is an ideal in R.

In $\mathbb{Z}$, $\mathbb{F}[x]$ every ideal has the form (a)

Over more general rings have to consider ideals like

Quotient Ring:

Let R be a commutative ring and $I \lhd R$ is an ideal.

Construct R/I w.r.t. additive structure on R

So elements of R/I are cosets

written $x + I$.

Rule of Equality

$$x + I = y + I$$

$$\Rightarrow x - y \in I$$

Group theory: $K \lhd G$ "K is normal to G"

Ring theory: $I \lhd R$ "I is an ideal in R"

Important!! Prop

If $I \lhd R$ then R/I is naturally a ring.

MATH 7202

03-03-17

<u>Proof</u>

I is a normal subgroup of the additive group R.
So R/I is naturally a group.

$$+ : R/I \times R/I \longmapsto R/I$$

$$(x + I) + (y + I) = x + y + I$$

So R/I is naturally an abelian (additive) group.

We want to construct a multiplication on R/I.

$$\bullet : R/I \times R/I \longmapsto R/I$$

$$(x + I) + (y + I) = x + y + I$$

Must show this is well defined.
i.e. if $x + I = x' + I$
and $y + I = y' + I$
then we have to show
$$xy + I = x'y' + I$$

$$xy - x'y' = xy - xy' + xy' - x'y'$$
$$= x(y - y') + (x - x')y'$$

$y - y' \in I$ so $x(y - y') \in I$ as I is an ideal
$x - x' \in I$ so $y'(x - x') \in I$ as I is an ideal
But R is commutative so $(x - x')y' \in I$.
so $xy - x'y' = x(y - y') + (x - x')y'$
So $xy - x'y' \in I$
so $xy + I = x'y' + I$
so $\bullet$ is well defined.

$I \triangleleft R \quad \therefore \quad R/I$

$(x+I)+(y+I) = x+y+I$
$(x+I)\cdot(y+I) = xy+I$

$\underline{0} = 0+I$
$\underline{1} = 1+I$
$(1+I)\cdot(x+I) = 1\cdot x + I = x+I$
So we have a ring. $\square$

<u>Examples</u>
$R = \mathbb{Z}$
Fix $n \in \mathbb{Z}$ $\quad (n \geq 2)$
$\mathbb{Z}/(n)$
$n = 5$
What do elements of $\mathbb{Z}/(5)$ look like?
$(5) = \{\mu 5 : \mu \in \mathbb{Z}\}$

$0+I,\ 1+I,\ 2+I,\ 3+I,\ 4+I,\ 5+I,\ 6+I, \ldots$

$5+I = 0+I \quad , \quad 5 = 5-0 \in I$
$6+I = 1+I$
$6-1 = 5 \in I$

$r+(5) = r+5q+(5)$
$r+5q-r = 5q \in (5)$
Repeat with period 5.

$\mathbb{Z}/(5) = \{0+(5),\ 1+(5),\ 2+(5),\ 3+(5),\ 4+(5)\}$
$= [0],\ [1],\ [2],\ [3],\ [4]$

MATH 7202

03-03-17

In $\mathbb{Z}/(n)$
write $[r] = r + (n)$

The elements of $\mathbb{Z}/(n)$ are
$[0], [1], \ldots, [n-1]$
$[r + nq] = [r]$

i.e. $\mathbb{Z}/(n)$ = arithmetic mod n
$= \mathbb{Z}/n$.

To multiply in $\mathbb{Z}/n$, multiply normally but every time you see n, replace by 0.

Multiplication in $\mathbb{Z}/3$:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$2 \cdot 2 = 4 = 1 + 3 = 1$

Multiplication in $\mathbb{Z}/4$

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$2 \times 2 = 4 = 0$
$2 \times 3 = 6 = 2 + 4 = 2$
$3 \times 3 = 9 = 1 + 2 \times 4 = 1$

$\mathbb{Z}/4$ is <u>not</u> a field
as 2 has no inverse.
2 is nilpotent.

$x \in R$ is called <u>nilpotent</u> when $x^n = 0$ for some n.

$\mathbb{Z}/5$

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}/5$ is a field, every non-zero element has an inverse.

$\mathbb{Z}/6$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Not a field.
$2 \times 3 = 0$ but $2 \neq 0$, $3 \neq 0$.

$\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime.

Def
R is a commutative ring.
Say that R is an integral domain iff $xy = 0 \Rightarrow x = 0$ or $y = 0$.

Similarly if $x \neq 0 \neq y$ then $xy \neq 0$.

Prop
Any field is an integral domain.

MATH 7202

03-03-17

Proof

Suppose $xy = 0$

and $x \neq 0$.

Multiply by x^{-1}:

$x^{-1}xy = x^{-1}\cdot 0 = 0$

$\Rightarrow y = 0$.

i.e. $xy = 0$ & $x \neq 0 \Rightarrow y = 0$

$\square$

Converse is false:

e.g.

$\mathbb{Z}$ is an integral domain but $\mathbb{Z}$ is not a field.

Prop

Let R be a finite commutative ring.

If R is an integral domain then R is a field.

Proof

Let $x \in R$, $x \neq 0$

Consider the mapping $\lambda : R \mapsto R$

given by $\lambda(y) = xy \quad (= yx)$.

λ is a homomorphism of additive groups

$\lambda : R \mapsto R$

$\lambda(y_1 + y_2) = x(y_1 + y_2) = xy_1 + xy_2$

$= \lambda(y_1) + \lambda(y_2)$

I claim that λ is injective.

$\lambda(y_1) = \lambda(y_2)$

$xy_1 = xy_2 \Rightarrow x(y_1 - y_2) = 0$

But $x \neq 0$.

Hence $y_1 - y_2 = 0 \Rightarrow y_1 = y_2$ (R integral domain)

So $\lambda(y_1) = \lambda(y_2) \Rightarrow y_1 = y_2$

$\lambda : R \mapsto R$ is injective, but R is finite so λ is bijective.
So $\exists y \in R, \ \lambda(y) = 1$
i.e. $\exists y \in R, \ xy = 1$
and x has an inverse.

$\square$

<u>Prop</u>
Let $n \in \mathbb{Z}$ $(n \geq 2)$
$\mathbb{Z}/n$ is an integral domain
$\Leftrightarrow$ n is prime.

<u>Proof</u>
First show: n is not prime $\Rightarrow$ $\mathbb{Z}/n$ is not an integral domain.
If n is not prime, write
$n = c \times d$, $0 < c < n$, $0 < d < n$.
So $[c] \neq 0$, $[d] \neq 0$
But $[c][d] = [cd] = [n] = 0$

Now suppose n is prime.
Suppose $[c][d] = 0$ where $[c] \neq 0$
i.e. c is <u>not</u> a multiple of n.
$[cd] = 0$ means $cd = \mu n$
$n \mid \mu n \Rightarrow n \mid cd$, n prime and $n \nmid c$
$\Rightarrow n \mid d$.
So $d = \lambda n \Rightarrow [d] = 0$
$[c][d] = 0$ and $[c] \neq 0$
$\Rightarrow [d] = 0$.

$\square$

MATH 7202

03-03-17

Theorem

Let $n \geq 2$, $n \in \mathbb{Z}$

The following satements are equivalent:

i). n is prime

ii). $\mathbb{Z}/n$ is an integral domain

iii). $\mathbb{Z}/n$ is a field

Proof

We've just shown (i) $\Leftrightarrow$ (ii)

As $\mathbb{Z}/n$ is finite (ii) $\Rightarrow$ (iii) by above

and (iii) $\Rightarrow$ (ii) is trivial.

$\square$

This is due to Gauss c. 1795

Galois generalised this c. 1829

$\mathbb{F}[t]/(p(t))$ where $(p(t)) = \{\mu(t)p(t) : \mu(t) \in \mathbb{F}[t]\}$

$\mathbb{F}_p = \mathbb{Z}/p$ only when p is prime.

$t^2 + t + 1 \in \mathbb{F}_2[t]$

How do we represent elements of

$\mathbb{F}_2[t]/t^2+t+1$?

Set $t^2 + t + 1 = 0$

$\cdot$	0	1	t	$1+t$
0	0	0	0	0
1	0	1	t	$1+t$
t	0	t	$1+t$	1
$1+t$	0	$1+t$	1	t

$t^2 = -t - 1 = 1 + t$

$t(1+t) = t + t^2 = -1 = 1$

$(1+t)(1+t) = t^2 + 2t + 1 = t$

MATH 7202

07-02-17

$\mathbb{Z}/n$ represent elements $\{0, 1, 2, \dots, n-1\}$

Euclidean algorithm $n \leq N$

$N = qn + r \qquad 0 \leq r \leq n-1$

$N - r \in (n) \quad$ so $[N] = [r]$

How about representing elements in

$\mathbb{F}[x]/p(x)$, $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

Still have a Euclidean algorithm

Suppose $b(x) = x^N + b_{N-1}x^{N-1} + \dots + b_1 x + b_0 \quad (n \leq N)$

Write $b(x) = q(x)p(x) + r(x)$

where $\deg(r) < \deg(p)$

$b(x) - r(x) \in (p(x))$

$[b(x)] = [r(x)] \in \mathbb{F}[x]/p(x)$

ie.

Prop

We can represent elements of $\mathbb{F}[x]/p(x)$

by polynomials $r(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \dots + c_1 x + c_0$

Corollary

If $p(x) \in \mathbb{F}[x]$ has $\deg p = n$ then

$\mathbb{F}[x]/p(x)$ is a vector space over $\mathbb{F}$

with basis $\{1, x, \dots, x^{n-1}\}$ and $\dim \mathbb{F}[x]/p(x) = n$

Example

$\mathbb{F}_2[x]/x^2+x+1$ This has dim 2 over $\mathbb{F}_2$

Basis elements: $\{1, x\}$

$\mathbb{F}_2[x]/x^2+x+1$ has 4 elements $\{0, 1, x, x+1\}$.

Addition is obvious

Multiplication

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Setting $x^2+x+1=0$

over $\mathbb{F}_2$ $x^2 \equiv x+1$

$(= -x-1)$ $\boxed{+1=-1}$

$x^2+x = -1 = 1$

$(x+1)^2 = x^2+2x+1 = x$

Prop

$\mathbb{F}_2[x]/x^2+x+1$ is a field

Proof

Look!

Every nonzero element has a multiplicative inverse. $\square$

Example

$\mathbb{F}_2[x]/x^2+1$

Still a vector space of dim 2 over $\mathbb{F}_2$

Still has 4 elements $\{0, 1, x, x+1\}$

$x^2+1 \equiv 0 \Rightarrow x^2 \equiv 1$

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

$x^2+x = 1+x$

$(x+1)^2 = x^2+2x+1$

$= 1+0x+1 = 0$

Corollary

$\mathbb{F}_2[x]/x^2+1$ is <u>not</u> a field

$x+1$ has no inverse!

MATH 7202

07-02-17

Over $\mathbb{F}_2$, $x^2+1 = (x+1)(x+1)$
but x^2+x+1 has no proper factorisation.

Def
$\mathbb{F}$ a field
$a(x) \in \mathbb{F}[x]$
$a(x) = a_n x^n + \dots + a_1 x + a_0$
with $a_n \neq 0$ i.e. $\deg a(x) = n$
Say that $a(x)$ has a proper factorisation over $\mathbb{F}$
when we can write $a(x) = b(x)\,c(x)$ where
$\deg(b) < n = \deg(a)$, $\deg(c) < n = \deg(a)$.

Def
If $p(x) \in \mathbb{F}[x]$ $\deg(p) \geq 1$
Say that $p(x)$ is irreducible over $\mathbb{F}$ when
$p(x)$ has no proper factorisation over $\mathbb{F}$.

For $\mathbb{Z}/n$, $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime
Thm
For $\mathbb{F}[x]/p(x)$, $\mathbb{F}[x]/p(x)$ is a field $\Leftrightarrow$ $p(x)$ is irreducible over $\mathbb{F}$.

Proof coming soon!

When is $p(x)$ irreducible over $\mathbb{F}$?
$\mathbb{F} = \mathbb{R}$
$p(x) = a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$
when is $p(x)$ irreducible over $\mathbb{R}$?

$\mathbb{F} = \mathbb{C}$
$p(x) = a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$ $(n \geq 1)$
$p(x)$ is irreducible $\Leftrightarrow$ $n = 1$
$p(x) = a_n (x-\lambda_1)\dots(x-\lambda_n)$

Over $\mathbb{R}$:

$p(x) = ax^2 + bx + c$

irred. $\Leftrightarrow$ $b^2 - 4ac < 0$

Polynomials over $\mathbb{Q}$?

Much more difficult.

For each $n \geq 1$ there are many more irreducibles of deg $= n$.

Eisenstein's Criterion coming soon!

$\mathbb{Q}[x]/x^2-2$ $\quad$ x^2-2 is irreducible $/\mathbb{Q}$

dim $\mathbb{Q}[x]/x^2-2$ has $\dim_{\mathbb{Q}} = 2$

basis $= \{1, x\}$ $\quad$ $x^2 - 2 \equiv 0 \Rightarrow x^2 \equiv 2.$

$(a+bx)(c+dx) = (ac + bdx^2) + (ad+bc)x$

$= ac + 2bd + (ad+bc)x$

If $x^2 = 2$, then $x = \sqrt{2}$

So $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad+bc)\sqrt{2}$

Example

$\mathbb{R}[x]/x^2+1$

$(a+bx)(c+dx)$ $\quad$ $x^2+1 \equiv 0 \Rightarrow x^2 \equiv -1$

$= (ac + bdx^2) + (ad+bc)x = (ac - bd) + (ad+bc)x$

here $x = i$ as $x^2 = -1$

Kronecker shows how to construct fields

MATH 7202

10 - 03 - 17

$\mathbb{F}[x]/a(x)$ $\mathbb{F}$ a field

$a(x) = a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$

w.l.o.g can suppose $a_n = 1$

$\hat{a}(x) = x^n + \left(\frac{a_{n-1}}{a_n}\right)x^{n-1} + \dots + \left(\frac{a_0}{a_n}\right)$

$(a(x)) = (\hat{a}(x))$

Take $a_n = 1$

$a(x)$ is monic

Recall if $a(x) \in \mathbb{F}(x)$, $\deg(a(x)) \geq 1$

$a(x)$ monic, can write

$a(x)$ as a product

$a(x) = b_1(x) b_2(x) \dots b_k(x)$, $k \leq \deg(a)$

$b_i(x)$ monic and irreducible

Factorisation is unique in the sence

$a(x) = c_1(x) \dots c_l(x)$,

$c_i(x)$ monic and irreducible,

then $k = l$ and $c_i(x) \equiv b_{\sigma(i)}(x)$ for some permutation σ.

Prop

$\mathbb{F}[x]/a(x)$, $a(x)$ monic, $\deg(a(x)) \geq 1$, $\mathbb{F}$ field.

Then $\mathbb{F}[x]/a(x)$ is an integral domain

$\Leftrightarrow$ $a(x)$ is irreducible over $\mathbb{F}$.

Proof

Suppose $a(x)$ is reducible, i.e. $a(x) = b(x)c(x)$

where $b(x), c(x) \in \mathbb{F}[x]$,

and $\deg(b) < \deg(a)$, $\deg(c) < \deg(a)$.

Consider

$[b(x)] \in \mathbb{F}[x]/a(x)$

$[c(x)] \in \mathbb{F}[x]/a(x)$

$[b(x)] \neq 0$, $[c(x)] \neq 0$, but

$[b(x)][c(x)] = [b(x)c(x)] = [a(x)] = 0$

So $\mathbb{F}[x]/a(x)$ is not an integral domain.

So $a(x)$ reducible $\Rightarrow$ $\mathbb{F}[x]/a(x)$ is not an integral domain.

$\therefore$ $\mathbb{F}[x]/a(x)$ integral domain $\Rightarrow$ $a(x)$ irreducible.

Conversely suppose $a(x)$ is irreducible
and that $[b(x)][c(x)] = 0$ in $\mathbb{F}[x]/a(x)$
i.e. $[b(x)c(x)] = 0$
So $b(x)c(x) = q(x)a(x)$ for some $q(x) \in \mathbb{F}[x]$
Write $b(x) = b_1(x) \dots b_k(x)$
$c(x) = c_1(x) \dots c_l(x)$, $b_i(x)$, $c_j(x)$ irreducible.

$q(x)a(x) = b_1(x) \dots b_k(x) c_1(x) \dots c_l(x)$
$a(x)$ is an irreducible factor on LHS.
By uniqueness we must have
either (i) $a(x) = b_i(x)$ for some i
or (ii) $a(x) = c_j(x)$ for some j

If (i): $b(x) = \lambda(x)a(x)$ for some $\lambda(x)$, $[b(x)] = 0$
If (ii): $c(x) = \mu(x)a(x)$ for some $\mu(x)$, $[c(x)] = 0$

i.e. $a(x)$ irreducible
$\Rightarrow [b(x)][c(x)] = 0 \Rightarrow [b(x)] = 0$ or $[c(x)] = 0$
So $a(x)$ irreducible $\Rightarrow$ $\mathbb{F}[x]/a(x)$ integral domain.
$\square$

MATH 7202

10-03-17

Comparison

$\mathbb{Z}/n$ integral domain $\Leftrightarrow$ n is prime

$\mathbb{F}[x]/a(x)$ integral domain $\Leftrightarrow$ $a(x)$ is irreducible (over $\mathbb{F}$)

We showed that $\mathbb{Z}/n$ integral domain $\Leftrightarrow$ $\mathbb{Z}/n$ is a field (used fact that $\mathbb{Z}/n$ is finite).

$\mathbb{F}[x]/a(x)$ is a vector space over $\mathbb{F}$.

$\dim = \deg(a(x)) = n$

Has basis $1, x, \dots, x^{n-1}$ $(n = \deg(a))$

$\mathbb{F}[x]/a(x)$ contains $\mathbb{F} = \{\lambda \cdot 1, \lambda \in \mathbb{F}\}$

Prop

Let A be an integral domain and suppose A contains a field $\mathbb{F}$ (as a subgroup) such that $\dim_{\mathbb{F}}(A)$ is finite. Then A is a field.

Proof

Assuming (i) A an integral domain,

(ii) $\dim_{\mathbb{F}}(A)$ is finite.

Let $a \in A$; $a \neq 0$.

Have to find $b \in A$ such that $ab = 1$

(i.e. $a \neq 0 \Rightarrow a$ has a multiplicative inverse)

Define $\lambda : A \longrightarrow A$ by $\lambda(x) = ax$.

λ is a linear map:

$\lambda(x+y) = a(x+y) = ax + ay = \lambda(x) + \lambda(y)$,

$\lambda(\xi x) = a\xi x = \xi a x = \xi \lambda(x)$ $\quad (\xi \in \mathbb{F})$.

Claim that:

$\mathrm{Ker}(\lambda) = 0$.

$\lambda(x) = ax = 0$

Since $a \neq 0$ and A an integral domain,

then $x = 0$.

So we can apply the Kernel - Rank Theorem:

($\dim A$ is finite)

$$\dim(\operatorname{Ker}\lambda) + \dim(\operatorname{Im}(\lambda)) = \dim A$$

But $\operatorname{Ker}(\lambda) = 0 \Rightarrow \dim(\operatorname{Im}\lambda) = \dim A$

So $\operatorname{Im}(\lambda) = A$,

so $1 \in \operatorname{Im}\lambda$

$\Rightarrow \exists\, b \in A$ such that $\lambda(b) = 1$,

$\exists\, b \in A \quad ab = 1$

So $a \neq 0 \Rightarrow \exists\, a^{-1} \in A$

i.e. A is a field.

$\square$

Corollary

Let $\mathbb{F}$ be a field, $a(x) \in \mathbb{F}[x]$, $\deg(a) \geq 1$.

The following statements are equivalent:

(i) $a(x)$ is irreducible over $\mathbb{F}$

(ii) $\mathbb{F}[x]/a(x)$ is an integral domain

(iii) $\mathbb{F}[x]/a(x)$ is a field.

Proof

(i) $\Leftrightarrow$ (ii) already done

(ii) $\Rightarrow$ (iii) because $\mathbb{F}[x]/a(x)$ is finite dimensional

(iii) $\Rightarrow$ (ii) is trivial.

$\square$

Beware: If A is an integral domain and $\dim_{\mathbb{F}}(A)$ is infinite then A need not be a field,

e.g. $A = \mathbb{F}[x]$.

MATH 7202

10-03-17

Question:

Given a field $\mathbb{F}$ and $a(x) \in \mathbb{F}[x]$, can we say anything about whether $a(x)$ is irreducible?

Example

$\mathbb{F} = \mathbb{C}$, $a(x) \in \mathbb{F}[x]$

"Fundamental Thm of Algebra"

$a(x) = C(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$

$n = \deg(a)$, λ_i, $C \in \mathbb{C}$.

Corollary

$a(x)$ monic.

$\mathbb{F} = \mathbb{C}$, $a(x) \in \mathbb{F}[x]$

$a(x)$ irreducible $\Leftrightarrow$ $\deg(a) = 1$.

ie. $a(x) = (x-\lambda)$ for some λ.

Example

$\mathbb{F} = \mathbb{R}$, $a(x) \in \mathbb{R}[x]$ monic.

Then there are two types of irreducible elements

(i) $a(x) = x - \lambda$ $(\lambda \in \mathbb{R})$

(ii) $a(x) = x^2 + bx + c$ $(b, c \in \mathbb{R}$, $b^2 - 4ac < 0)$

Proof

$a(x) \in \mathbb{R}[x]$ (monic)

$\mathbb{R} \subset \mathbb{C}$

$a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, $a_i \in \mathbb{R}$

Factorise $a(x)$ over $\mathbb{C}$

$a(x) = (x-\lambda_1)\dots(x-\lambda_n)$, $\lambda_i \in \mathbb{C}$

$\bar{a}(x) = x^n + \sum_{i=0}^{n-1} \bar{a}_i x^i$

$\bar{a}_i = a_i$ $\Rightarrow$ $\bar{a}(x) = a(x)$

Suppose λ is a root of $a(x)$

$a(\lambda) = 0$

Then $\bar{a}(\bar{\lambda}) = 0$

and $\bar{\lambda}$ is a root of $\bar{a}(x) = a(x)$

So in factorisation of $a(x)$

$$a(x) = (x-\lambda_1)\cdots(x-\lambda_k)(x-\mu_1)(x-\bar{\mu}_1)\cdots(x-\mu_m)(x-\bar{\mu}_m)$$

$n = k + 2m$ and $\mu_i, \bar{\mu}_i$ are not real.

but $\lambda_1, \ldots, \lambda_k$ are real.

Write $\mu_r = \xi_r + i\eta_r$, $\bar{\mu}_r = \xi_r - i\eta_r$, $\eta_r \neq 0$

$$[x-(\xi+i\eta)][x-(\xi-i\eta)]$$
$$= x^2 + 2\xi x + (\xi^2+\eta^2)$$
$$(2\xi)^2 - 4(\xi^2+\eta^2) = -4\eta^2 < 0$$

as $\eta \neq 0$

$$a(x) = (x-\lambda_1)\cdots(x-\lambda_k)\prod_{r=1}^{m}(x^2+b_r x + c_r), \quad b_r^2 - 4c_r < 0.$$

Irreducible polynomials over $\mathbb{Q}$

If $a(x) \in \mathbb{Q}[x]$, then for some positive integer, K, I can suppose $Ka(x) \in \mathbb{Z}[x]$

$a(x) = \sum\left(\frac{d_r}{q_r}\right)x^r$, put $K = \prod q_r$.

We might as well consider polynomials over $\mathbb{Z}[x]$.

We are interested in polynomials $a(x) \in \mathbb{Z}[x]$ which have no proper factorisation over $\mathbb{Z}$

i.e. $a(x) = b(x)c(x)$ then either $b(x)$ or $c(x)$ is a constant.

Eisenstein's Criterion

Let p be a prime

$a(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_i \in \mathbb{Z}$

Then $a(x)$ has no proper factorisation provided the following three conditions are satisfied:

MATH 7202

10-03-17

(i) $a_n \not\equiv 0 \pmod{p}$
(ii) $a_r \equiv 0 \pmod{p}$ for $0 \leq r \leq n-1$
(iii) $a_0 \not\equiv 0 \pmod{p^2}$

Examples

$$x^{15} + 3x^7 + 9x^4 + 27x^3 + 6$$

has no proper factorisation over $\mathbb{Z}$

$p = 3$

$x^{101} + 82x^{57} + 164x^3 + 41$, $p = 41$

Whereas if I take $x^4 + x^3 + x^2 + x + 1$,
this doesn't satisfy Eisenstein's Criterion immediately,
however...

Suppose $f(x) = b(x)c(x)$

$\lambda \in \mathbb{F}$ consider

$g(x) = f(x+\lambda)$ If f is a polynomial of deg $= n$, so is g.

$f(x+\lambda) = b(x+\lambda)c(x+\lambda)$

write $d(x) = b(x+\lambda)$, $e(x) = c(x+\lambda)$

So $g(x) = d(x)e(x)$

Prop

Let $f(x) \in \mathbb{F}[x]$ and write $g(x) = f(x+\lambda)$, $\lambda \in \mathbb{F}$

$f(x)$ has no proper factorisation

$\Leftrightarrow$ $g(x)$ has no proper factorisation.

$f(x) = x^4 + x^3 + x^2 + x + 1$

$g(x) = f(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$

$= (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$

$f(x)$ has no proper factorisation over $\mathbb{Z}$ because
$g(x)$ does not have proper factorisation, $p = 5$

Factorise $x^n - 1$ into irreducibles over $\mathbb{Q}$

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

__Prop__

If p is prime then

$$c_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$$

has no proper factorisation over $\mathbb{Z}$.

__Proof__

$$c_p(x) = \frac{x^p - 1}{x - 1}$$

$$c_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{(x+1)^p - 1}{x}$$

$$(x+1)^p = x^p + \sum_{r=1}^{p-1} \binom{p}{r} x^r + 1$$

$$(x+1)^p - 1 = x^p + \sum_{r=1}^{p-1} \binom{p}{r} x^r$$

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + \sum_{s=0}^{p-2} \binom{p}{s+1} x^s$$

All $\binom{p}{s+1} \equiv 0 \mod p$

$\binom{p}{0+1} = \binom{p}{1} = 1 \not\equiv 0 \mod p^2$

So $c_p(x+1)$ satisfies Eisenstein's Criterion with prime p.

__Prop__

$$x^{p-1} + x^{p-2} + \dots + x + 1$$

is irreducible over $\mathbb{Q}$

when p is prime.

False when p is not prime.

MATH 7202

10-03-17

Example

$$x^4 - 1 = (x-1)(x^3 + x^2 + x + 1)$$
$$= (x^2-1)(x^2+1) = (x-1)(x+1)(x^2+1)$$
$$\Rightarrow (x^3 + x^2 + x + 1) = (x+1)(x^2+1)$$

reducible!

Theorem (Eisenstein)

Let p be a prime.

$a(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \in \mathbb{Z}[x]$

and suppose that

(i) $a_n \not\equiv 0 \pmod p$

(ii) $a_r \equiv 0 \pmod p \qquad 0 \le r \le n-1$

(iii) $a_0 \not\equiv 0 \pmod{p^2}$

Then $a(x)$ has no proper factorisation over $\mathbb{Z}$.

Proof

Suppose $a(x) = b(x)c(x)$

$b(x) = b_k x^k + \dots + b_1 x + b_0$,

$c(x) = c_m x^m + \dots + c_1 x + c_0 \qquad , \quad b_i, c_j \in \mathbb{Z}$

with $b_k \neq 0$, $c_m \neq 0$

and suppose $k < n$, $m < n$ (proper factorisation)

Multiply out and compare coefficients.

Constants: $a_0 = b_0 c_0$

$a_0 \equiv 0 \bmod p$ but $a_0 \equiv 0 \bmod p^2$

So either $b_0 \equiv 0 \pmod p$, $c_0 \not\equiv 0 \pmod p$

or $b_0 \not\equiv 0 \pmod p$, $c_0 \equiv 0 \pmod p$.

W.l.o.g suppose $b_0 \not\equiv 0 \pmod p$, $c_0 \equiv 0 \pmod p$.

Coefficient of x: $a_1 = b_1 c_0 + b_0 c_1$

$a_1 \equiv 0 \pmod p$, $b_1 c_0 \equiv 0 \pmod p$

So $b_0 c_1 \equiv 0 \pmod p$

But $b_0 \not\equiv 0 \pmod{p}$ so $c_1 \equiv 0 \pmod{p}$

Claim that $c_r \equiv 0 \pmod{p}$ $\forall r$ s.t. $0 \leq r \leq k$.

By induction:
Suppose true for $\leq r-1$.
Look at coefficient of x^r.

$$a_r = b_0 c_r + b_1 c_{r-1} + \dots + b_r c_0$$
$$= b_0 c_r + \sum_{s=0}^{r-1} b_{r-s} c_s$$

$a_r \equiv 0 \pmod{p}$ $(r \leq k \leq n)$
$\Rightarrow$ RHS $\equiv 0 \pmod{p}$
Also $c_s \equiv 0 \pmod{p}$ $s \leq r-1$
$\Rightarrow b_0 c_r \equiv 0 \pmod{p}$
but $p \nmid b_0 \Rightarrow c_r \equiv 0 \pmod{p}$
(Completes induction)

So for $0 \leq r \leq m$,
$c_r \equiv 0 \pmod{p}$
Now look at coefficients of x^n
$a_n \equiv b_k c_m$
$a_n \not\equiv 0 \pmod{p}$, $c_m \equiv 0 \mod p$
※ contradiction.
So assumption that $a(x)$ has proper factorization is false. $\square$

MATH 7202

14-03-17

Eisenstein's Criterion

$a(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$, $a_r \in \mathbb{Z}$

If p is prime and $a_n \not\equiv 0 \mod p$, $a_r \equiv 0 \mod p$ for $0 \le r \le n-1$, and $a_0 \not\equiv 0 \mod p^2$,

then $a(x)$ has no proper factorisation over $\mathbb{Z}$.

i.e. we can't write $a(x) = b(x)d(x)$

where $\deg(b) < \deg(a) = n$ and $\deg(d) < \deg(a) = n$,

$b(x), d(x) \in \mathbb{Z}[x]$.

Question:

If $a(x) \in \mathbb{Z}[x]$ has no proper factorisation over $\mathbb{Z}$, does it have a proper factorisation over $\mathbb{Q}$?

NO

Def

Suppose $a(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

Define $C(a) = HCF\{a_0, a_1, \dots, a_n\}$ ← Content of $a(x)$

Gauss' Lemma

Let $b(x), d(x) \in \mathbb{Z}[x]$ and suppose $C(b) = C(d) = 1$

then $C(bd) = 1$.

Proof

Let $e(x) = e_m x^m + \dots + e_1 x + e_0$ $(e_r \in \mathbb{Z})$

Then $C(e) = 1$ precisely when given any prime p, $\exists r : p \nmid e_r$.

Suppose $\left.\begin{aligned} b(x) &= b_m x^m + \dots + b_1 x + b_0 \\ d(x) &= d_n x^n + \dots d_1 x + d_0 \end{aligned}\right\} \in \mathbb{Z}[x]$

and $C(b) = 1$, $C(d) = 1$.

Choose a prime p.

Put $k = \min\{r : p \nmid b_r\}$

$l = \min\{s : p \nmid d_s\}$.

I claim that p does not divide the coefficient of x^{k+l} in $b(x)d(x)$.

Note that p divides b_r $(r<k)$
and p divides d_s $(s<l)$.

Coefficient of x^{k+l} in $b(x)d(x)$ is

$$b_k d_l + \sum_{r=1}^{k} b_{k-r} d_{l+r} + \sum_{s=1}^{l} b_{k+s} d_{l-s}$$

p divides $\sum_{r=1}^{k} b_{k-r} d_{l+r}$, $k-r<k$

p divides $\sum_{s=1}^{l} b_{k+s} d_{l-s}$, $l-s<l$

But p does not divide $b_k d_l$ by choice of k, l.

So given any prime p, $\exists$ at least one coefficient in $b(x)d(x)$ which is coprime to p.

So $C[b(x)d(x)] = 1$. $\square$

Suppose $\beta(x) \in \mathbb{Q}[x]$

$$\beta(x) = \sum_{r=0}^{n} \left(\frac{\xi_r}{\eta_r}\right) x^r \quad , \quad \xi_r, \eta_r \in \mathbb{Z}$$

Put $D = LCM(\eta_0, \ldots, \eta_r)$

?

$$D\beta(x) = \sum_{r=0}^{n} \xi_r \mu_r x^r \quad \text{where } \frac{\mu_r}{D} = \eta_r \quad , \mu_r \in \mathbb{Z}$$

Put $N = HCF\{\xi_r \mu_r\}$

$D\beta(x) = N b(x)$ where $b(x) \in \mathbb{Z}[x]$ and $C(b) = 1$

So $\beta(x) = \left(\frac{N}{D}\right) b(x)$ [where $b(x) \in \mathbb{Z}[x]$ $C(b) = 1$]

MATH 7202

14-03-17

Prop

Let $a(x) \in \mathbb{Z}[x]$ with $C(a) = 1$
If $a(x)$ has no proper factorisation over $\mathbb{Z}$,
then $a(x)$ has no proper factorisation over $\mathbb{Q}$.

Proof

Suppose $a(x) = \beta(x)\delta(x)$ is a proper factorisation over $\mathbb{Q}$, so $\deg\beta < \deg a$, $\deg\delta < \deg a$,
$\beta(x), \delta(x) \in \mathbb{Q}[x]$.

Write $\beta(x) = \left(\frac{N_1}{D_1}\right) b(x)$, $\delta(x) = \left(\frac{N_2}{D_2}\right) d(x)$, ($N_i$, D_i integers)

where $b(x), d(x) \in \mathbb{Z}[x]$, $C(b) = C(d) = 1$.

$\deg(b) = \deg(\beta) < \deg(a)$

$\deg(d) = \deg(\delta) < \deg(a)$

$$a(x) = \left(\frac{N_1 N_2}{D_1 D_2}\right) b(x)d(x)$$

$D_1 D_2\, a(x) = N_1 N_2\, b(x)d(x)$.

By hypothesis $C(1) = 1$, so content of LHS $= D_1 D_2$.
By Gauss' Lemma, $C(bd) = 1$, so content of RHS $= N_1 N_2$.
So $D_1 D_2 = N_1 N_2$
and $a(x) = b(x)d(x)$ is a proper factorisation of $a(x)$ over $\mathbb{Z}$. ⨳ contradiction.

$\square$

Corollary

If $a(x) \in \mathbb{Z}[x]$ has no proper factorisation over $\mathbb{Z}$ then $a(x)$ has no proper factorisation over $\mathbb{Q}$.

Proof

Write $a(x) = C(a)\,\alpha(x)$, $C(\alpha) = 1$.
Then $\alpha(x)$ also has no proper factorisation over $\mathbb{Z}$.
Suppose $a(x) = \beta(x)\delta(x)$ is a proper factorisation of $a(x)$ over $\mathbb{Q}$.

Write $\tilde{\beta}(x) = \frac{1}{C(a)} \beta(x) \quad \in \mathbb{Q}[x]$

$\alpha(x) = \tilde{\beta}(x)\delta(x)$ is a proper factorisation over $\mathbb{Q}$. ⋇ contradiction (previous result).

$\square$

Most general form of Eisenstein's Criterion:

Theorem

Let $a(x) = a_n x^n + \dots + a_1 x + a_0$, $a_r \in \mathbb{Z}$

Suppose for some prime p

(i) $a_n \not\equiv 0 \mod p$

(ii) $a_r \equiv 0 \mod p$

(iii) $a_0 \not\equiv 0 \mod p^2$

Then $a(x)$ has no proper factorisation over $\mathbb{Q}$, i.e. $a(x)$ is irreducible over $\mathbb{Q}$.

If asked in exam Eisenstein $\Rightarrow$ only the integer part!

Proof

By Gauss' Lemma $C(bd) = 1$

so content of RHS $= N_1 N_2$,

so $D_1 D_2 = N_1 N_2$ and $a(x) = b(x)d(x)$ is a proper factorisation of $a(x)$ over $\mathbb{Z}$.

⋇ contradiction

$\square$

Ring homomorphisms & ring isomorphisms

Suppose $R = (R, +, 0, \cdot, 1_R)$, $S = (S, +, 0, \cdot, 1_S)$

Let $\varphi : R \mapsto S$ be a mapping.

Say φ is a ring homomorphism when

(i) $\varphi : (R, +, 0) \mapsto (S, +, 0)$ is a homomorphism of abelian groups, i.e. $\varphi(x+y) = \varphi(x) + \varphi(y)$.

(ii) $\forall x, y \in R$, $\varphi(xy) = \varphi(x)\varphi(y)$

(iii) $\varphi(1_R) = 1_S$.

MATH 7202

14-03-17

Say that φ is a ring isomorphism when φ is also bijective.

Let $R_1 = (R_1, +, 0, \cdot, 1)$, $R_2 = (R_2, +, 0, \cdot, 1)$ be rings.

By $R_1 \times R_2$ I mean the ring whose underlying set is $R_1 \times R_2$.

Addition: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$

$0 = (0, 0)$

Multiplication: $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$

$1 = (1, 1)$

$R_1 \times R_2$ is a ring.

Prop

Let m, n be positive integers

If m, n are coprime

$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$

Proof

Define $\mu : \mathbb{Z}/mn \mapsto \mathbb{Z}/m$ $\qquad \mu[x]_{mn} = [x]_m$

$\nu : \mathbb{Z}/mn \mapsto \mathbb{Z}/n$ $\qquad \nu[x]_{mn} = [x]_n$

Then $\mu \times \nu : \mathbb{Z}_{mn} \mapsto \mathbb{Z}/m \times \mathbb{Z}/n$ is a ring homomorphism

$\mu \times \nu$ is injective : $Ker(\mu \times \nu) = (0, 0)$

why? : $(\mu \times \nu)[x] = (0, 0)$

i.e. $[x]_m = 0$ & $[x]_n = 0$

i.e. $x = mq$, $x = ns$

$\Rightarrow mq = ns$, but m, n coprime

so $m \mid s$ and $n \mid q$.

So $s = \sigma m$, $q = \tau n$.

$x = mq = mn\tau$ so $[x]_{mn} = 0$

So $\ker(\mu \times \nu) = 0$, $\mu \times \nu$ injective.

$\mu \times \nu : \mathbb{Z}/_{m,n} \hookrightarrow \mathbb{Z}/_m \times \mathbb{Z}/_n$

injective,

both sides have mn elements

$\Rightarrow \mu \times \nu$ bijective

So $\mathbb{Z}/_{mn} \cong \mathbb{Z}/_m \times \mathbb{Z}/_n$

$\square$

MATH 7202

17-03-17

Aut (C_N) ?

$C_N = \{1, x, \dots, x^{N-1}\}$

? Aut$(C_N) \leftrightarrow \{r : 0 \le r \le N-1,\ r \text{ coprime to } N\}$

$\mathbb{Z}/_N = \{r : 0 \le r \le N-1\}$ no conditions

For any commutative ring R,

$R^* = \{x \in R : \exists y \in R,\ xy = yx = 1\}$

Sometimes write

$R^* = \mathcal{U}(R) \leftarrow$ unit group

R^* is a group under multiplication.

If R is a field, $R^* = R - \{0\}$

but if R is not a field, $R^* \subsetneq R - \{0\}$

Prop

Aut$(C_N) \cong (\mathbb{Z}/_N)^*$

Proof

Consider the mapping

$(\mathbb{Z}/_N)^* \longrightarrow \text{Aut}(C_N)$

$a \longmapsto \varphi_a$

$\varphi_a(x) = x^a \qquad (C_N = \{1, x, \dots, x^{N-1})$

$\square$

Last time we saw

$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$

provided m, n are coprime

Prop

If R_1, R_2 are rings then

$(R_1 \times R_2)^* = R_1^* \times R_2^*$

Proof

Let $(x,y) \in R_1 \times R_2$ and $(w,z) \in R_1 \times R_2$.

$(w,z)\cdot(x,y) = (wx, zy)$

$(x,y)\cdot(w,z) = (xw, yz)$

(x,y) is invertible when $\exists\ (w,z) \in R_1 \times R_2$

s.t. $(w,z)\cdot(x,y) = (1,1) = 1_{R_1 \times R_2}$

$(x,y)\cdot(w,z) = (1,1)$ //

i.e. when $xw = wx = 1$ and $zy = yz = 1$

$\Rightarrow$ $x \in R_1^*$ and $y \in R_2^*$

So $(x,y) \in (R_1 \times R_2)^* \Leftrightarrow x_1 \in R_1^*$ and $y \in R_2^*$

$\square$

How about $(\mathbb{Z}/n)^*$?

Write N as a product of prime powers,

$N = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$

where $p_1, \dots, p_m$ are distinct primes.

Prop

$\mathbb{Z}/N \cong \mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_2^{e_2} \times \dots \times \mathbb{Z}/p_m^{e_m}$.

Proof

$m=1$: nothing to prove.

$m=2$: $N = p_1^{e_1} p_2^{e_2}$

$p_1^{e_1}, p_2^{e_2}$ are coprime so $\mathbb{Z}/p_1^{e_1}p_2^{e_2} \cong \mathbb{Z}/p_1^{e_1} \times \mathbb{Z}/p_2^{e_2}$

Suppose true for $m-1$, put $L = p_1^{e_1} \dots p_{m-1}^{e_{m-1}}$, $K = p_m^{e_m}$

L, K are coprime, $LK = N$.

So $\mathbb{Z}/N \cong \mathbb{Z}/L \times \mathbb{Z}/K$

By induction $\mathbb{Z}/L = \mathbb{Z}/p_1^{e_1} \times \dots \times \mathbb{Z}/p_1^{e_1}$, $\mathbb{Z}/K = \mathbb{Z}/p_m^{e_m}$,

so $\mathbb{Z}/p_1^{e_1} \dots p_m^{e_m} \cong \mathbb{Z}/p_1^{e_1} \times \dots \times \mathbb{Z}/p_m^{e_m}$

$\|$

$\mathbb{Z}/N$ $\square$

MATH 7202

17-03-17

How big is $(\mathbb{Z}/N)^*$?

Euler's "Totient Function":

$$\Phi(N) = |(\mathbb{Z}/N)^*|$$

[Latin: Quotiens - How many?
Totiens - So many!]

So $|Aut(C_N)| = \Phi(N)$

Prop
If $N = p_1^{e_1} \cdots p_m^{e_m}$ and $p_1, \dots, p_m$ are distinct primes.
$\Phi(N) = \Phi(p_1^{e_1})\Phi(p_2^{e_2}) \cdots \Phi(p_m^{e_m})$

Proof
$(\mathbb{Z}/N)^* \cong (\mathbb{Z}/p_1^{e_1})^* \times \dots \times (\mathbb{Z}/p_m^{e_m})^*$

$\square$

So to calculate $\Phi(N)$ it is enough to calculate $\Phi(p^e)$

Prop
If p is prime, $\Phi(p^e) = (p-1)p^{e-1}$.

Proof
The non units in $\mathbb{Z}/p^e$ are the residues which are divisible by p.
How many non units?
Non units $= \{mp : 0 \le m \le p^{e-1}\}$
$|\text{Non units}| = p^{e-1}$
So $(\mathbb{Z}/p^e)^* = p^e - p^{e-1} = (p-1)p^{e-1}$

$\square$

Example

$|(\mathbb{Z}/10^6)^*| = \Phi(10^6)$

$10^6 = 2^6 5^6$

$\Phi(10^6) = \Phi(2^6)\,\Phi(5^6)$

$= 2^5 \times (5-1)\,5^5$

$= 400,000 = 4 \times 10^5$

So C_{10^6} has $400,000$ automorphisms.

So we know how big $\mathrm{Aut}(C_N)$ is.
We don't know what the group structure is.

Simplest case

$N = p$, prime.
We'll show:

Theorem

$\mathrm{Aut}(C_p) \cong C_{p-1}$

This is a special case of a more general theorem.

Theorem:

Let $\mathbb{F}$ be a field and let $G \subset \mathbb{F}^*$ be a finite subgroup. Then G is cyclic.

Special case:

$G \subset \mathbb{F}^*$ and $|G| = p^n$, p prime.
Then $G \cong C_{p^n}$ (so G is cyclic).

Proof

As $|G| = p^n$, if $g \in G$ then $\mathrm{ord}(g) = p^e$ where $e \leq n$.
Define $\exp(G) = \max\{k : \exists g \in G,\ \mathrm{ord}(g) = p^k\}$

MATH 7202

17-03-17

Put $e = \exp G$, then $e \le n$.
Suppose $e < n$.
Then every $g \in G$ ($\subset \mathbb{F}$) satisfies the equation $x^{p^e} - 1 = 0$.

As $\mathbb{F}$ is a field this equation has at most p^e solutions.
However $\forall g \in G$ g is a solution and $|G| = p^n$.
So $|G| = p^n \le p^e \le p^n = |G|$
So $e = n$ contradiction.
Hence $n = \max\{k : \exists g \in G, \ ord(g) = p^n\}$
i.e. $\exists g \in G$ $ord(g) = p^n$
$|G| = p^n$ so G is cyclic.

□ (Special case)

<u>General case:</u>

$G \subset \mathbb{F}^*$ is a finite subgroup.
Suppose $|G| = p_1^{e_1} \cdots p_m^{e_m}$, $p_1, \ldots, p_m$ distinct primes.
Then G is cyclic.

<u>Proof:</u> (By induction on m)
$m = 1$: already done.
By Sylow, for each i, $\exists$ a subgroup G_i with $|G_i| = p_i^{e_i}$.
For each r define
$G(r) = G_1 G_2 \cdots G_r$ $(\subset G)$
Claim that for each r
$G(r)$ is a subgroup of G
and $G(r) \cong G_1 \times \ldots \times G_r$.
$r = 1$: nothing to prove
Suppose proved for $r-1$
$G(r) = G(r-1) G_r$.

$G(r-1)$ is a subgroup (by inductive hypothesis)
G_r normalises $G(r-1)$ (G is abelian)
$G(r-1) \cap G_r = \{1\}$
Coprime orders.
$G(r) \cong G(r-1) \rtimes G_r$ (by Recognition Criterion)
But $G(r)$ is abelian.
So the semidirect product is simply a direct product,

$$G(r) \cong G(r-1) \times G_r.$$

By induction

$$G = G_1 \times \dots \times G_m$$

Each G_i is cyclic

$$G_i \cong C_{p_i^{e_i}}$$

Factors have coprime order so

$$G \cong C_{p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}} \text{ is cyclic.}$$

□

$G \subset \mathbb{F}^*$ finite subgroup
G is cyclic.

<u>First case</u>

Take $\mathbb{F} = \mathbb{F}_p$ (field with p elements)
$(\mathbb{F}_p)^*$ is finite
$|(\mathbb{F}_p)^*| = p-1$.

<u>Corollary</u>

$$\mathbb{F}_p^* \cong C_{p-1}$$

<u>Corollary</u>

$$\mathrm{Aut}(C_p) \cong C_{p-1}$$

<u>Proof</u>

$$\mathrm{Aut}(C_p) \cong \mathbb{F}_p^*.$$

□

MATH 7202

17-03-17

See 3rd year course "Galois Theory"

[Galois proved for each prime p, integer $n \geq 1$,
$\exists$ unique (up to isomorphism) field $\mathbb{F}$,
$|\mathbb{F}_p| = p^n$
For such a field, $\mathbb{F}^* = C_{p^n - 1}$]

$(\mathbb{Z}/p^e)^* = C_{p-1} \times C_{p^{e-1}}$ (except when $p = 2$)

$|(\mathbb{Z}/p^e)^*| = (p-1)p^{e-1}$

$(\mathbb{Z}/8)^* \cong C_2 \times C_2$
$(\mathbb{Z}/16)^* \cong C_2 \times C_4$
$(\mathbb{Z}/2^{n+1})^* \cong C_2 \times C_{2^n - 1}$
(See Dr Hill's Number Theory courses)

Factorisation of $x^n - 1$ over $\mathbb{Q}$

Factorise $x^n - 1$ over $\mathbb{C}$ by putting
$\zeta = \exp\left(\frac{2\pi i}{n}\right)$
$x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{n-1})$

Prop
$$x^n - 1 = \prod_{r=0}^{n-1} (x - \zeta^r), \quad \zeta = \exp\left(\frac{2\pi i}{n}\right)$$

$\{1, \zeta, \ldots, \zeta^{n-1}\} \cong C_n$
so $\operatorname{ord}(\zeta^k)$ divides n.
Define
$$C_r(x) = \prod_{\operatorname{ord}(\zeta^k) = n} (x - \zeta^k), \quad r \mid n.$$
?

So $x^n - 1 = \prod_{r \mid n} C_r(x)$.

On the face of it the factors $C_r(x)$ don't look too helpful, however they are easily computable.

$C_1(x) = x - 1$

$x^2 - 1 = C_1(x) C_2(x) = (x-1) C_2(x)$

$\Rightarrow C_2(x) = x + 1$

$x^3 - 1 = C_1(x) C_3(x) = (x-1) C_3(x) \Rightarrow C_3(x) = x^2 + x + 1.$

$x^4 - 1 = C_1(x) C_2(x) C_4(x) = (x^2 - 1) C_4(x) \Rightarrow C_4(x) = x^2 + 1$

$x^6 - 1 = C_1(x) C_2(x) C_3(x) C_6(x) = (x^3 - 1) C_2 C_6$

$\Rightarrow C_2 C_6 = x^3 + 1 \Rightarrow C_6(x) = x^2 - x + 1$

$C_1(x) = x - 1$

$C_2(x) = x + 1$

$C_3(x) = x^2 + x + 1$

$C_4(x) = x^2 + 1$

$C_5(x) = x^4 + x^3 + x^2 + x + 1$

$C_6(x) = x^2 - x + 1$

<u>Example</u>

Factorise $x^{12} - 1$

$x^{12} - 1 = C_1 C_2 C_3 C_4 C_6 C_{12}$

$= (x^6 - 1) C_4 C_{12}$

$\Rightarrow C_4 C_{12} = x^6 + 1$

$\Rightarrow C_{12}(x) = (x^6 + 1) / (x^2 + 1) = x^4 - x^2 + 1$

$\therefore x^{12} - 1 = (x-1)(x+1)(x^2 + x + 1)(x^2 + 1)(x^2 - x + 1)(x^4 - x^2 + 1)$

MATH 7202

21-03-17

$$x^n - 1 = \prod_{r|n} c_r(x)$$

How about $x^n + 1$?

Observe $x^{2n} - 1 = (x^n - 1)(x^n + 1)$

$$\prod_{r|2n} c_r(x) = \prod_{r|n} c_r(x) \prod_{\substack{r|2n \\ r\nmid n}} c_r(x)$$

Prop

$$x^n + 1 = \prod_{\substack{r|2n \\ r\nmid n}} c_r(x)$$

Example

$x^{12} + 1$

factorise $x^{24} - 1 = c_1 c_2 c_3 c_4 c_6 c_8 c_{12} c_{24}$

$x^{12} - 1 = c_1 c_2 c_3 c_4 c_6 c_{12}$

$\Rightarrow x^{12} + 1 = c_8 c_{24}$

$c_8 = x^4 + 1$ as $\underbrace{x^8 - 1}_{c_1 c_2 c_4 c_8} = \underbrace{(x^4 - 1)}_{c_1 c_2 c_4}\underbrace{(x^4 + 1)}_{c_8}$

$x^{12} + 1 = c_8 c_{24}$

$\Rightarrow c_{24} = \dfrac{x^{12} + 1}{x^8 + 1} = x^8 - x^4 + 1$

$\Rightarrow x^{12} + 1 = (x^4 + 1)(x^8 - x^4 + 1)$

$= c_2(x^2)\, c_3(-x^4)$

$C_r(x) = \prod(\zeta - 1)$

ζ is a primitive r^{th} root of unity

$C_r(x)$ irreducible over $\mathbb{Q}$ (Galois Theory)

MATH 7202
PC

21-03-17

Hw 8

3). $\mathbb{F}[x]/_{x^2-1} \cong \mathbb{F} \times \mathbb{F}$

provided 2 is invertible

<u>General method</u>

$\mathbb{Z}/_{mn} \cong \mathbb{Z}/_m \times \mathbb{Z}/_n$ provided m, n are coprime

$\Updownarrow$

$\mathbb{F}[x]/_{p(x)q(x)} \cong \mathbb{F}[x]/_{p(x)} \times \mathbb{F}[x]/_{q(x)}$

provided $p(x), q(x)$ have no common factor.

$$\mathbb{F}[x]/_{p(x)q(x)} \xrightarrow{\varphi(x)} \mathbb{F}[x]/_{p(x)} \times \mathbb{F}[x]/_{q(x)}$$

s.t.

$$[\alpha]_{pq} \longmapsto ([\alpha]_p, [\alpha]_q)$$

is a ring homomorphism.

When is φ injective?

$\varphi(\alpha) = (0, 0)$

$$\Rightarrow \begin{cases} [\alpha]_p = 0 & \alpha(x) = p(x) f(x) \\ [\alpha]_q = 0 & \alpha(x) = q(x) g(x) \end{cases}$$

$\alpha(x) = p(x) f(x) = q(x) g(x)$

Suppose p, q coprime $\Rightarrow p(x) \mid g(x)$, $q(x) \mid f(x)$.

If $([\alpha]_p, [\alpha]_q) = (0, 0)$

$\Leftrightarrow \alpha(x) = p(x) q(x) \tilde{f}(x)$

$\Leftrightarrow [\alpha]_{pq} = 0$

Suppose $p(x), q(x)$ are coprime,

$\mathbb{F}[x]/_{p(x)q(x)} \longmapsto \mathbb{F}[x]/_{p(x)} \times \mathbb{F}[x]/_{q(x)}$

$[\alpha]_{pq} \longmapsto ([\alpha]_p, [\alpha]_q)$ injective and linear

$\dim LHS = \deg p(x)q(x)$ $\qquad$ $\dim RHS = \deg p + \deg q$

$= \deg p(x) + \deg q(x)$

So if $p(x)$, $q(x)$ coprime

$\phi : \mathbb{F}[x]/p(x)q(x) \xrightarrow{\cong} \mathbb{F}[x]/p(x) \times \mathbb{F}[x]/q(x)$
is an injective linear map between spaces of same dimension.

<u>Specific case</u>
If 2 invertibe on $\mathbb{F}$
$x^2-1 = (x-1)(x+1)$
$x-1$, $x+1$ coprime
$\mathbb{F}[x]/x^2-1 \xrightarrow{\cong} \mathbb{F}[x]/x-1 \times \mathbb{F}[x]/x+1 \cong \mathbb{F} \times \mathbb{F}$
But $\mathbb{F}[x]/x-1 \cong \mathbb{F} \cong \mathbb{F}[x]/x+1$.

<u>Elementary method</u>
How can you tell when R is a product
$R \cong R_1 \times R_2$?

In $R_1 \times R_2$ $\quad 1 = (1,1)$, $1^2 = 1$
Put $\varepsilon_1 = (1,0)$ $\quad \varepsilon_2 = (0,1)$

$\varepsilon_1^2 = (1,0)^2 = (1,0) = \varepsilon_1$
$\varepsilon_2^2 = \varepsilon_2$
$\varepsilon_1 + \varepsilon_2 = 1$
$\varepsilon_2 \varepsilon_1 = \varepsilon_1 \varepsilon_2$

Suppose 2 is invertible
$\mathbb{F}[x]/x^2-1 = \{a+bx \mid a,b \in \mathbb{F}\}$ $\quad x^2=1$
Try to solve $\varepsilon^2 = \varepsilon$ in the above.
$(a+bx)^2 = (a^2+b^2x^2) + 2abx$ $\quad x^2 = 1$
$= a^2+b^2 + 2abx$

$\varepsilon = a+bx$
$\varepsilon^2 = \varepsilon \iff a = a^2+b^2$, $b = 2ab$.

MATH 7202
PC
21-03-17

Suppose $b \neq 0$
Then $a = \frac{1}{2}$

$$\Rightarrow \frac{1}{2} - \frac{1}{4} = b^2 \Rightarrow b^2 = \frac{1}{4} \Rightarrow b = \pm\frac{1}{2}$$

Two solutions: $\varepsilon_1 = \frac{1}{2}(1+x)$, $\varepsilon_2 = \frac{1}{2}(1-x)$

$$\begin{aligned}
\mathbb{F}\times\mathbb{F} &\longmapsto \mathbb{F}[x]/x^2-1\\
(1,0) &\longmapsto \varepsilon_1\\
(0,1) &\longmapsto \varepsilon_2\\
(a,b) &\longmapsto a\varepsilon_1 + b\varepsilon_2\\
&= \frac{a}{2}(1+x) + \frac{b}{2}(1-x)
\end{aligned}$$

Define
$\varphi : \mathbb{F}\times\mathbb{F} \xrightarrow{\cong} \mathbb{F}[x]/x^2-1$
$\varphi(a,b) = \frac{1}{2}(a+b + (a-b)x)$
φ is a ring isomorphism.

$\mathbb{F} = \mathbb{R}$
$\mathbb{R}[x]/x^2-a$
If $a > 0$ $\sqrt{a} \in \mathbb{R}$

$$\begin{aligned}
x^2-a &= (x-\sqrt{a})(x+\sqrt{a})\\
&= a\left(\frac{x}{\sqrt{a}} - 1\right)\left(\frac{x}{\sqrt{a}} + 1\right)
\end{aligned}$$

Put $y = \frac{x}{\sqrt{a}}$

$$x^2 - a = a(y-1)(y+1) = a(y^2-1)$$

$$\mathbb{R}[x]/x^2-a \cong \mathbb{R}[y]/y^2-1 \overset{a\neq 0}{\cong} \mathbb{R}\times\mathbb{R}.$$

So $\mathbb{R}[x]/x^2-a \cong \mathbb{R}\times\mathbb{R}$
when $a>0$.

When $a<0$, put $b=-a$, $b>0$.

$\mathbb{R}[x]/x^2-a \equiv \mathbb{R}[x]/x^2+b$
$\sqrt{b} \in \mathbb{R}$, $b>0$
put $y = \frac{x}{\sqrt{b}}$

$\mathbb{R}[x]/x^2+b \cong \mathbb{R}[y]/y^2+1 \cong \mathbb{C}$

So $\mathbb{R}[x]/x^2-a = \begin{cases} \mathbb{R}\times\mathbb{R} & a>0 \\ \mathbb{C} & a<0. \end{cases}$

$\mathbb{R}[x]/x^2$
$x^2=0$, $x\neq 0$
If R is a ring $\lambda\in R$
λ is nilpotent when $\lambda^n=0$ for some n.

$\mathbb{R}[x]/x^2$ is not a field as x is nilpotent

$\lambda^n=0$ $\nexists\mu$ s.t. $\lambda\mu=1$

$\lambda^n\mu^n=1$, $\lambda^n\mu^n=0$, $1\neq 0$.

MATH 7202

24-03-17

Revison class:
Monday April 24
JZ Young LT
3 - 5 pm

$\varphi : G \longmapsto H$, G, H groups
$\Gamma \subset G$, Γ a subgroup of G
?: $\varphi(\Gamma)$ is a subgroup of H

$1 \in \varphi(\Gamma)$ $\varphi(1) = 1$
$x, y \in \varphi(\Gamma)$
write $x = \varphi(a)$, $y = \varphi(b)$
$a, b \in \Gamma$ so $ab \in \Gamma$
So $xy = \varphi(a)\varphi(b) = \varphi(ab)$
So $xy \in Im(\Gamma)$
$x \in \varphi(\Gamma)$, $x = \varphi(a)$ $a \in \Gamma$, $a^{-1} \in \Gamma$
$\varphi(a^{-1}) = x^{-1}$ so $x^{-1} \in \varphi(\Gamma)$
So $\varphi(\Gamma)$ is a subgroup of H.

Classify groups of order 28.
$28 = 2 \times 2 \times 7 = 7 \times 2^2$
(Hint: try the largest prime first) $|G| = 28$
Sylow tells us G has at least one subgroup K s.t. $|K| = 7$ and at least one subgroup Q s.t. $|Q| = 4$.
Also if N_7 = no. of subgroups of order 7,
$N_7 \equiv 1 \mod 7$
So either $N_7 = 1$, or $N_7 \geq 8$.
We get a contradiction if $N_7 \geq 8$.
Why?

Suppose $K_1, \dots, K_8$ are distinct subgroups
s.t. $|K_i| = 7$
$K_i \neq K_j$ if $i \neq j$.
So $K_i \cap K_j = \{1\}$ if $i \neq j$
If $\gamma \in K_i \cap K_j$, $\gamma \neq 1$
Then $K_i = \{1, \gamma, \gamma^2, \dots, \gamma^6\}$
and $K_j = \{1, \gamma, \dots, \gamma^6\}$
So $K_i = K_j \Rightarrow$ contradiction.
So $N_7 = 1$
i.e. K is the unique subgroup of order 7
so $K \lhd G$.
Why?
If $g \in G$
gKg^{-1} is also a subgroup of order 7.
So $gKg^{-1} = K$ (uniqueness)
We know G has a subgroup Q, $|Q| = 4$
$K \cap Q = \{1\}$ (coprime orders)
and $|G| = |K||Q|$
So $G \cong K \rtimes_h Q$ where $K \cong C_7$
$|Q| = 4$, $h : Q \longmapsto Aut(C_7)$ is some homomorphism.
Two possibilities for Q.
I). $Q \cong C_4$
II). $Q \cong C_2 \times C_2$
$C_7 = \{1, x, \dots, x^6\}$, $x^7 = 1$
$C_4 = \{1, y, y^2, y^3\}$, $y^4 = 1$
$C_2 \times C_2 = \{1, s, t, st\}$, $s^2 = 1 = t^2$, $st = ts$
I). $h : C_4 \mapsto Aut(C_7) \cong C_6 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$
orders: 1 6 3 2 3 6

Two possibilities for h
a). $h(y) = 1$
b). $h(y) = \alpha^3$ so $h(y)(x) = x^6 = x^{-1}$

MATH 7202

24-03-17

a). $C_7 \rtimes_h C_4 \quad h(y) = Id$

$\cong C_7 \times C_4 \cong C_{28}$

b). $h(y)(x) = x^6$

$\langle X, Y \mid X^7 = 1, Y^4 = 1 \rangle \leftarrow D_{14}^*$ or $Q(28)$

$YX = X^6 Y = X^{-1} Y \qquad [YXY^{-1} = X^{-1}]$

If you call $G = D_{14}^*$ this is the binary dihedral group of order 28.

If you call $G = Q(28)$ this is the quaternionic group of order 28.

I). $G \cong C_{28}$ or D_{14}^*

II). ? $\quad Q = C_2 \times C_2$

$h : C_2 \times C_2 \longmapsto Aut(C_7) = C_7 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$

Four possibilities for h.

0). $h(s) = 1, \quad h(t) = 1, \quad h(st) = 1 \qquad$ (trivial)

$\Rightarrow G \cong C_7 \times C_2 \times C_2 \cong C_{14} \times C_2$

i). $h(1) = 1, \quad h(s) = \alpha^3, \quad h(t) = 1, \quad h(st) = \alpha^3$

ii). $h(1) = 1, \quad h(s) = 1, \quad h(t) = \alpha^3, \quad h(st) = \alpha^3$

iii). $h(1) = 1, \quad h(s) = \alpha^3, \quad h(t) = \alpha^3, \quad h(st) = 1$

i), ii) and iii) all give the same group $D_{14} \times C_2$

i). $\langle X, S, T \mid X^7 = 1, S^2 = 1, T^2 = 1, TS = ST,$
$SX = X^6 S = X^{-1} S, \; SXS^{-1} = X^{-1} \rangle$

Here $(X, S) \leftrightarrow D_{14}$

$(T) \longleftrightarrow C_2 \qquad$ so $D_{14} \times C_2$

ii). Similar, $(X, T) \longleftrightarrow D_{14}, \quad (S) \longleftrightarrow C_2 \qquad$ so $D_{14} \times C_2$

iii). $(X, S) \leftrightarrow D_{14}, \quad (ST) \leftrightarrow C_2 \qquad$ so $D_{14} \times C_2$

So: I). $G \cong C_{28}$ or D_{14}*

II). $G \cong C_{14} \times C_2$

or $G \cong D_{14} \times C_2$

Def

A finite group G is called simple when G has no normal subgroups except $\{1\}$ and G.

i). C_p is simple for each prime p.

ii). Smallest non abelian simple group is A_5

$|A_5| = 60$ (even permutations on $\{1, \ldots, 5\}$)

iii). Next largest has order $= 168$

(invertible 3×3 matrices over $\mathbb{F}_2$)

iv). Except for C_p, any group divisible by only 2 primes is not simple (Burnside c1903)

v). If you know all finite simple groups then in principle you can construct all finite groups.

vi). Can we classify all finite simple groups?

Lyons, Aschbacher, Gorenstein.

$R = \mathbb{F}_2[x] / x^2 + x + 1$ $\qquad 0, 1, x, x+1$

$\varphi : R \mapsto R$

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

$\varphi_1(x) = x$, $\varphi_1(x+1) = x+1$ $\qquad \varphi_1 = Id$

$\varphi_2(x) = x+1$, $\varphi_2(x+1) = x$, $\varphi_2^{\,2} = Id$

$Aut(R) = C_2$