

7202 Algebra 4: Groups and Rings Notes

Based on the 2011 spring lectures by Prof F E A
Johnson

The Author has made every effort to copy down all the content on the board during lectures. The Author accepts no responsibility what so ever for mistakes on the notes or changes to the syllabus for the current year. The Author highly recommends that reader attends all lectures, making his/her own notes and to use this document as a reference only.

Revision

Defn $G = (G, *, e) \rightarrow$ group

- set \downarrow element of set: $e \in G$
- 1) $*$: $G \times G \rightarrow G$ mapping \rightarrow associative
- 2) $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$ } ab-law DeMorgan's
- Identity \rightarrow 3) $a * e = e * a = a \quad \forall a \in G$
- 4) $\forall a \exists a^{-1} : a * a^{-1} = e = a^{-1} * a \quad \rightarrow$ Inverses

Identity
neqmpa...
a...um

In practice: we use either:

- Multiplicative convention $\left\{ \begin{array}{l} * = \cdot \\ e = 1 \\ a^{-1} = a^{-1} \end{array} \right.$ \rightarrow upabucuo

- Additive convention $\left\{ \begin{array}{l} * = + \\ e = 0 \\ a^{-1} = -a \end{array} \right.$ \rightarrow Note: used only when $a+b = b+a$ commutative

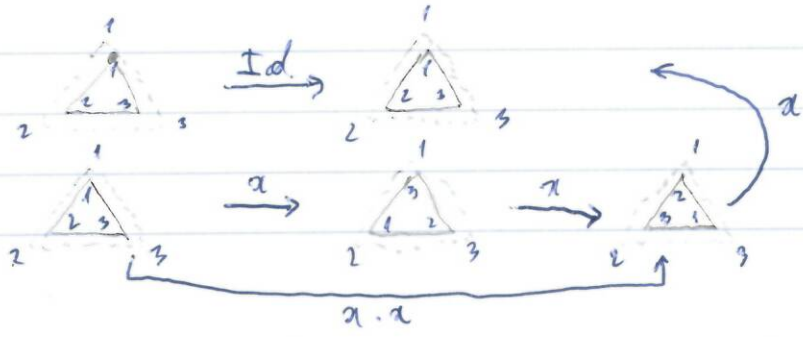
We use this very little, as most groups are not Abelian!

So: $G = (G, *, 1) \quad 1 \in G \quad G \neq \emptyset$, i.e. group is not empty set.

Example 1 C_3 cyclic group of order 3



Symmetries of 1-sided Δ .



conclusion : $\{1, x, x^2\} \leftarrow$ Discr. of group
 $x^3 = 1$

C_3	1	x	x^2
1	1	x	x^2
x	x	x^2	$\cancel{x}1$
x^2	x^2	$\cancel{x}1$	x

\leftarrow "Latin Square"

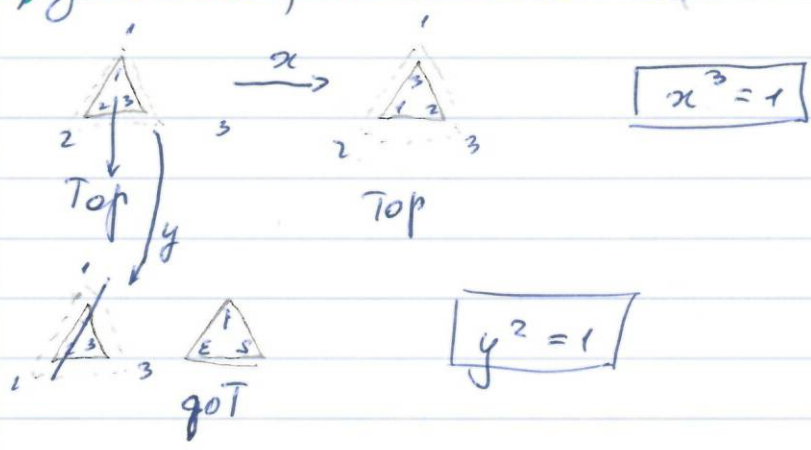
$x \cdot x = x \cdot x$

$x \cdot x^2 = x^2 \cdot x$

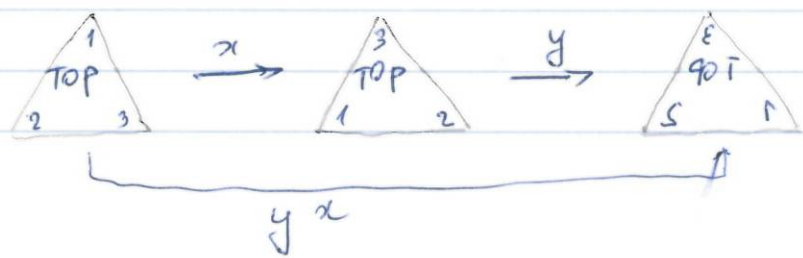
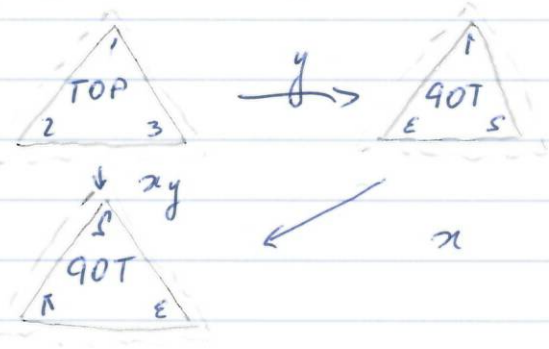
$x^2 \cdot x^2 = x^2 \cdot x^2$ commutative

Abelian.

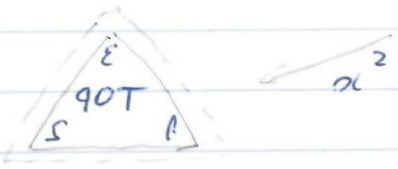
2) Symmetries of a 2-sided Δ



$fo g =$ first g then f
 $xy =$ first y then x



So $yx \neq xy$



So $yx = x^2y$

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

D_6	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	xy	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

D_6 = symmetry group of 2 sided Δ .
= Dihedral group

↓
Two dimensional symmetry

yx^2 we know $yx = x^2y$
 $yx^2 = yxx = x^2yx = x^2 \cdot x^2y = xy$
 $(yxy) = x^2y \cdot y = x^2$
 $(yx^2y) =$

So far

C_3 = group of symmetries of 1 sided equilateral Δ
is abelian

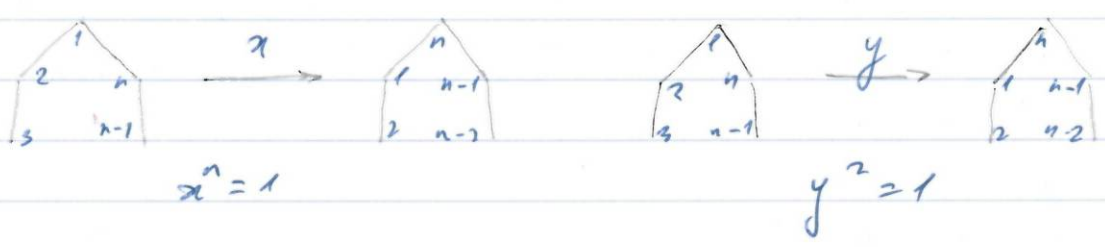
D_6 = " " " " " " " "
6 = 2 x 3 Non-abelian

generalisation:

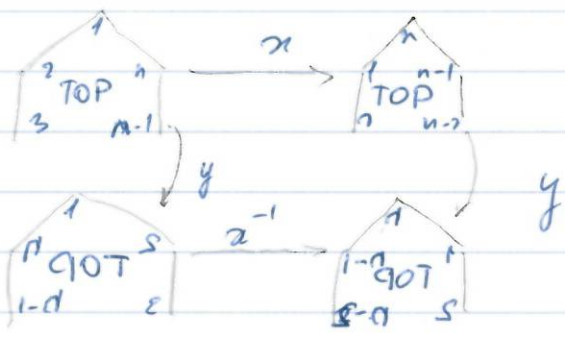
14/01/11

- 1) $C_n = \{1, \alpha, \dots, \alpha^{n-1}\}$ $\alpha^n = 1$ - cyclic group of order n
 (o) $\alpha =$ rotation through $\frac{2\pi}{n}$ (anticlockwise)
 (o) $\alpha^{-1} = \alpha^{n-1}$ (o) $\alpha \alpha^{n-1} = \alpha^n = 1$

- 2) $D_{2n} =$ Dihedral group of order $2n = \{1, \alpha, \dots, \alpha^{n-1}, y, \alpha y, \dots, \alpha^{n-1} y\}$ $\alpha^n = 1, y^2 = 1$
 (o) $\alpha =$ rotate regular 2 -sided n -gen. through $\frac{2\pi}{n}$
 TOP \rightarrow TOP
 (o) $y =$ flip about chosen vertex
 TOP \rightarrow BOT



Q. How do α, y interact?



this shows $y\alpha = \alpha^{-1}y$, alternatively expressed $y\alpha = \alpha^{n-1}y$
 $\alpha^{-1} = \alpha^{n-1}$

$D_{2n} = \{1, \alpha, \dots, \alpha^{n-1}, y, \alpha y, \dots, \alpha^{n-1} y\}$
 (o) $\alpha^n = 1, y^2 = 1, y\alpha = \alpha^{n-1}y$

symmetric isomorphism

Quaternion group of order 8: Q_8

$\{1, i, -1, -i\}$
 $i^2 = -1, i^3 = -i, i^4 = 1$
 This is another model for C_4

$Q_8 = \{1, i, -i, j, -j, k, -k\}$
 $i^2 = -1, j^2 = -1, k^2 = -1$
 $k = ij = -ji$

W. R. Hamilton 1850

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

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

non-abelian group
 and symmetric assoc.
 amicable?

Q_8 nonabelian group of order 8
 D_8 nonabelian gr. of order 8

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

$D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, yx = x^3y \rangle$

C_4	1	x	x^2	x^3		1	i	-1	$-i$
1	1	x	x^2	x^3	1	1	i	-1	$-i$
x^4	x^4	x^2	x^3	x^1	i	i	-1	$-i$	1
x^2	x^2	x^3	1	x^4	-1	-1	$-i$	1	i
x^3	x^3	1	x	x^2	$-i$	$-i$	1	i	-1

Conclusion: Q_8 & D_8 are essentially different ^{isomorphic} _{non-isomorphic}

→ Defn. Let $G = (G, \cdot, 1_G)$ & $K = (K, *, 1_K)$ be groups
 say that a mapping $f: G \rightarrow K$ is a **group homomorphism** when
 $f(g_1 g_2) = f(g_1) * f(g_2)$ for all $g_1, g_2 \in G$

- Ex. $\mathbb{R} = (\mathbb{R}, +, 0)$
 $\mathbb{R}_+ = (\mathbb{R}_+, \cdot, 1)$ $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$
- $\exp: \mathbb{R} \rightarrow \mathbb{R}_+$ is homomorphism, as $\exp(x+y) = \exp(x) \exp(y)$
 - $\log: \mathbb{R}_+ \rightarrow \mathbb{R}$ is homomorphism
 $\log(xy) = \log x + \log y$
 - $\text{sign}(\sigma\tau) = \text{sign}(\sigma) \text{sign}(\tau)$

Defn. We write $G \cong K$ when \exists **bijective homomorphism** $f: G \rightarrow K$
 G and K are then **isomorphic**

Note that in D_8 , $1, a^2, y, xy, a^2y, a^2xy$ are all self inverse whereas in Q_8 only $1, -1$ are self inverse

Elementary properties of homomorphism

$G = (G, \cdot, 1_G)$
 $H = (H, +, 1_H)$

- 1) $f(1_G) = 1_H$
- 2) $f(x^{-1}) = f(x)^{-1}$

$f: G \rightarrow H$ group homomorphism
 $f(x)^{-1}$ is inverse of element
 $f^{-1}(x)$ is inverse function
 $f(x)^{-1} f(x) = 1$
 $f^{-1}(f(x)) = x$

Proof of (1)

$f(1_G) = f(1_G \cdot 1_G) = f(1_G) + f(1_G)$
 multiply (on left) by $f(1_G)^{-1}$

$$f(1_G)^{-1} + f(1_G) = f(1_G)^{-1} + f(1_G) + f(1_G)$$

$$1_H = 1_H + f(1_G) = f(1_G)$$

→ this is inverse of element $f(1_G)$ in H

Q.E.D. (1)

Proof of (2)

$1_G = a \cdot a^{-1} = a^{-1} \cdot a$
 $f(1_G) = f(a \cdot a^{-1}) = f(a) + f(a^{-1})$

But $f(1_G) = 1_H$

so $f(a) + f(a^{-1}) = 1_H$

Similarly $f(a^{-1}) + f(a) = 1_H$

so $f(a^{-1}) = (f(a))^{-1}$

Q.E.D.

- 3) If $f: G \rightarrow H$ is a bijective homomorphism, then $f^{-1}: H \rightarrow G$ is also a homomorphism.

Proof of (3)

We know f^{-1} exists (f bijective)

let $h_1, h_2 \in H$

Need to show: $f^{-1}(h_1 * h_2) = f^{-1}(h_1) * f^{-1}(h_2)$

Note $f(f^{-1}(h_1 * h_2)) = (f \circ f^{-1})(h_1 * h_2) = \text{id}(h_1 * h_2) = h_1 * h_2$

Also $f(f^{-1}(h_1) * f^{-1}(h_2)) = f \circ f^{-1}(h_1) * f \circ f^{-1}(h_2) = h_1 * h_2$

f is homomorphism

So $f[f^{-1}(h_1 * h_2)] = f[f^{-1}(h_1) * f^{-1}(h_2)]$

But f is injective

□ So $f^{-1}(h_1 * h_2) = f^{-1}(h_1) * f^{-1}(h_2)$ Q.E.D

Application: $\mathbb{Q}_8 \cong \mathbb{D}_8$

Suppose $f: G \rightarrow K$ is bijective homomorphism
suppose that $x \in G$ satisfies $x \cdot x = 1_G$, then
 $f(x \cdot x) = f(x) * f(x) = 1_K$

Let $S(G) = \{x \in G : x \cdot x = 1_G\}$
 $S(K) = \{y \in K : y * y = 1_K\}$

induces
 if introduced a mapping
 $f: S(G) \rightarrow S(K)$
 Let $f^{-1}: S(K) \rightarrow S(G)$

[e.g. $f: S(G) \rightarrow S(K)$ is bijective with inverse
 $f^{-1}: S(K) \rightarrow S(G)$]

If $\mathbb{Q}_8 \cong \mathbb{D}_8$

Then \exists bijection
 $S(Q_8) \rightarrow S(D_8)$

But $|S(Q_8)| = 2$ $|S(D_8)| = 8$

so $Q_8 \not\cong D_8$ Q.E.D.

korany lemma
sufficiently finite to $r \rightarrow \infty$

generalisation

→ Defn

let G be a finite group, and
 $g \in G$
 $\text{ord}(g) = \min \{ r \in \mathbb{N} : g^r = 1 \}$

- e.g. $D_6 = \{ 1, \alpha, \alpha^2, g, g\alpha, \alpha^2g \}$
- $\text{ord}(1) = 1$
 - $\text{ord}(\alpha) = 3$
 - $\text{ord}(\alpha^2) = 3$
 - $\text{ord}(g) = 2$
 - $\text{ord}(g\alpha) = 2$
 - $\text{ord}(g\alpha^2) = 2$

$\text{ord}(g) \mid |D_6|$ where $g \in D_6$
→ korany?

$v_n(G) = |\{ g \in G : \text{ord}(g) = n \}|$

e.g. for $G = D_6$
 $v_1(D_6) = 1$, $v_2(D_6) = 3$, $v_3(D_6) = 2$, $v_n(D_6) = 0$ for $n \geq 4$

$D_8 = \{ 1, \alpha, \alpha^2, \alpha^3, g, \alpha g, \alpha^2 g, \alpha^3 g \}$
orders 1 4 2 4 2 2 2 2

$Q_8 = \{ 1, -1, i, -i, j, -j, k, -k \}$
orders 1 2 4 4 4 4 4 4

$$\nu_1(D_8) = 1, \nu_2(D_8) = 1, \nu_3(D_8) = 0, \nu_4(D_8) = 2, \nu_n(D_8) = 0 \quad n \geq 5$$

$$\nu_1(Q_8) = 1, \nu_2(Q_8) = 1, \nu_3(Q_8) = 0, \nu_4(Q_8) = 6, \nu_n(Q_8) = 0 \quad n \geq 5$$

To Do exercises 1 & 2.

You need to prove:

Prop. let $f: G \rightarrow K$ be a bijective homomorphism

Then f induces a bijection

$$f: G(n) \rightarrow K(n) \quad \text{for each } n$$

where $G(n) = \{x \in G : \text{ord } x = n\}$

$$K(n) = \{y \in K : \text{ord } y = n\}$$

$$\text{so } \nu_n(G) = |G(n)| \quad \nu_n(K) = |K(n)|$$

$$\text{so } \dots \nu_n(G) = \nu_n(K)$$

Directly

NFE

Prop. if $[G \& K \text{ are isomorphic } (G \& K \text{ are groups})]$

$$\Rightarrow [\text{ord } g = \text{ord } f(g)]$$

where $f(g)$ is associated bijectively uniquely element in K and $g \in G$.

Proof: to order maximum.

Corollary if $[G \& K \text{ are isomorphic}] \Rightarrow [\nu_n(G) = \nu_n(K)]$

Direct product of groups

Def-n $G = (g_i, \cdot_g)$ $H = (h_i, \cdot_h)$ } is a group itself
 $G \times H = (g \times h, \cdot)$
 $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot g_2, h_1 \cdot h_2)$

e.g. $C_3 \times C_3$ $C_3 = \{1, \alpha, \alpha^2\}$

$\{ (1,1), (\alpha,1), (\alpha^2,1), (1,\alpha), (\alpha,\alpha), (\alpha^2,\alpha), (1,\alpha^2), (\alpha,\alpha^2), (\alpha^2,\alpha^2) \}$
1 3 3 3 3 3 3 3 3

$C_9 = \{1, y, y^2, y^3, y^4, y^5, y^6, y^7, y^8\}$
1 3 3 3 3 3 3 3 3

$\text{ord}(y) = 9$ $\text{ord}(C_3 \times C_3) = 9$

18.01.11

$C_8 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$ $\alpha^8 = 1$

$\text{ord}(1) = 1$ $\text{ord}(\alpha) = 8$ $\text{ord}(\alpha^2) = 4$ $\text{ord}(\alpha^3) = 8$
 $\text{ord}(\alpha^4) = 2$ $\text{ord}(\alpha^5) = 8$ $\text{ord}(\alpha^6) = 4$ $\text{ord}(\alpha^7) = 8$

$\text{ord}(\alpha^a)$ div 8

Question: $C_n = \{1, \alpha, \dots, \alpha^{n-1}\}$ $\alpha^n = 1$

A typical element is α^r

what is $\text{ord}(\alpha^r)$?

A: $\text{ord} \alpha^r = \frac{n}{\text{HCF}(n,r)}$

where α is just α in $C_n = \{1, \alpha, \dots, \alpha^{n-1}\}$

Proposition: let $\alpha^N \in C_n$ ($N \geq 1$)
 if $\alpha^N = 1$, then n div. N if $\alpha^N \in H$ ($N \geq 1$)
 if $\alpha^N = 1 \Rightarrow \text{ord} \alpha \mid N$

Proof: $\text{ord}(\alpha) = n = \min \{r : \alpha^r = 1\}$ and $\alpha^N = 1$ then by def-n $n \mid N$

2) Div: $n = qn + r$ ($0 \leq r < n$)

$$1 = a^N = a^{qn+r} = a^{qn} a^r = (a^n)^q a^r$$

But $a^n = 1$ so $a^r = 1$ and $0 \leq r < n$

If $r \neq 0$ get contradiction (def. of min)

□ so $r = 0$ $N = qn$ QED

Prop. $\text{ord}(a^r) = \frac{n}{\text{HCF}(n, r)}$

Proof. Write $\text{ord}(a^r) = k$

$$\text{so } (a^r)^k = 1, \text{ so } a^{rk} = 1$$

hence n div. rk

ie. rk is a multiple of n

rk is obviously a multiple of r .

So rk is common multiple of n, r

when k is minimised $(a^n)^k = 1$ ($k \geq 1$)

then rk is lowest common multiple of n and r .

$$\text{so } r \text{ ord } a^r = \text{LCM}(n, r) = \frac{nr}{\text{HCF}(n, r)}$$

$$\text{so } \text{ord } a^r = \frac{n}{\text{HCF}(n, r)}$$

QED

Prop. let $f: G \rightarrow K$ $g: K \rightarrow K$ be a group homomorphism

then $g \circ f: G \rightarrow K$ is also a homomorphism

Proof: $(g \circ f)(a_1 a_2) = g(f(a_1 a_2))$

$$= g[f(a_1) f(a_2)] = g[f(a_1)] g[f(a_2)]$$

$$= (g \circ f)(a_1) (g \circ f)(a_2) \quad \text{Q.E.D.}$$

Automorphism group of G :

Defn Let G be a group
 A mapping $\alpha: G \rightarrow G$ is called **automorphism** of G , when

(1) α is a homomorphism
 (2) α is bijective.

Defn. $\text{Aut}(G) = \{ \alpha: G \rightarrow G \text{ s.t. } \alpha \text{ is an automorphism} \}$

claim: $\text{Aut}(G)$ is itself a group.

\Rightarrow **Proof:**

Multiplication on $\text{Aut}(G)$:

- $\text{Aut}(G) \times \text{Aut}(G) \rightarrow \text{Aut}(G)$
- $(\alpha, \beta) \rightarrow \alpha \circ \beta$
- $\Rightarrow \circ$ is binary operation

is it bijective? \forall
 $\alpha \circ \beta(a) = \alpha(\beta(a)) \Rightarrow \alpha = \text{id} \forall$
 $(\forall a \in G \exists \alpha \in G \text{ s.t. } \alpha \circ \beta(a) = a) \forall$
 composition and is associative

Prop. if $\alpha, \beta \in \text{Aut } G$ then $\alpha \circ \beta \in \text{Aut } G$

Proof: composition of homomorphism is homomorphism

\square " " of bijective mapping is bijective
 $\Rightarrow \circ$ is binary operation

Identity: Take $\text{Id}_G: G \rightarrow G$

(done) **Inverses:** If $\alpha: G \rightarrow G$ is bijective homomorphism, then

- (1) α^{-1} is bijective and
- (2) α^{-1} is a homomorphism

so $\alpha^{-1} \in \text{Aut}(G)$

binary operation * a map is v.s.t.
 $S \times S \rightarrow S$

\square Composition is always associative so get a group \square

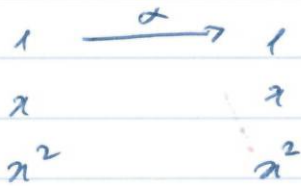
Example:

Determine $\text{Aut}(C_3)$

$$C_3 = \{1, \alpha, \alpha^2\} \quad \alpha^3 = 1$$

Let $\alpha \in \text{Aut}(C_3)$

$$\alpha(1) = 1$$



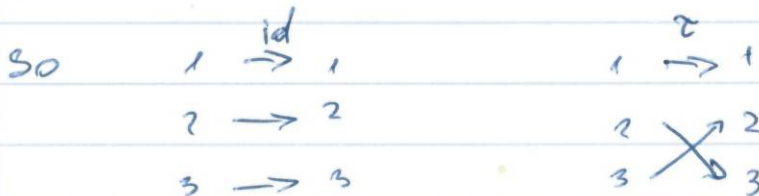
what are possibilities for $\alpha(\alpha)$?

either $[\alpha(\alpha) = \alpha]$, then $\alpha(\alpha^2) = \alpha(\alpha)\alpha(\alpha) = \alpha \cdot \alpha = \alpha^2$
and then $\alpha = \text{id}$

OR $[\alpha(\alpha) = \alpha^2]$, then $\alpha(\alpha^2) = \alpha$ by bijectivity

$$\left. \begin{array}{l} \alpha(\alpha^2) = \alpha = \alpha^2 \cdot \alpha^2 = \alpha(\alpha)\alpha(\alpha) \\ \alpha(\alpha^2 \cdot \alpha^2) = \alpha(\alpha) = \alpha^2 = \alpha(\alpha)\alpha(\alpha^2) \\ \alpha(\alpha \cdot \alpha^2) = \alpha(1) = 1 \\ \alpha(\alpha)\alpha(\alpha^2) = \alpha^2 \cdot \alpha = 1 \end{array} \right\}$$

is a permutation,
and a permutation
is a bijective map
isomorphism



$$\text{Aut}(C_3) = \{\text{Id}, \tau\}$$

where $\tau(\alpha) = \alpha^2$ $C_3 = \{1, \alpha, \alpha^2\}$
 $\tau(\alpha^2) = \alpha$

what is $\tau \circ \tau$

$$(\tau \circ \tau)(\alpha) = \tau(\tau(\alpha)) = \tau(\alpha^2) = \alpha$$

$$(\tau \circ \tau)(\alpha^2) = \tau(\tau(\alpha^2)) = \tau(\alpha) = \alpha^2$$

so $\tau \circ \tau = \text{Id}$

$$\text{Aut}(C_3) \cong C_2$$

	1	σ
1	1	σ
σ	σ	1

$$2) \text{Aut}(C_5) = C_5 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\} \quad \alpha^5 = 1$$

1	\rightarrow	1	How many choices for α ? A: At most 4.
α		α	
α^2		α^2	
α^3		α^3	
α^4		α^4	

Prop: It is enough to say where α takes α

Proof: Suppose

$$\begin{aligned} \alpha(\alpha) &= \alpha^a \\ \alpha(\alpha^2) &= \alpha(\alpha)\alpha(\alpha) = \alpha^a \alpha^a = \alpha^{2a} \\ \alpha(\alpha^3) &= \alpha^{3a} \\ \alpha(\alpha^4) &= \alpha^{4a} \end{aligned}$$

Let $\gamma: C_5 \rightarrow C_5$

$$\begin{aligned} \gamma(1) &= 1 \\ \gamma(\alpha) &= \alpha^a \\ \gamma(\alpha^2) &= \alpha^{2a} \\ \gamma(\alpha^3) &= \alpha^{3a} \\ \gamma(\alpha^4) &= \alpha^{4a} \\ \gamma(\alpha^5) &= 1 \end{aligned}$$

$$\begin{aligned} \gamma^2(\alpha) &= \gamma(\gamma(\alpha)) = \alpha^{a^2} \\ \gamma^3(\alpha) &= \gamma(\gamma^2(\alpha)) = \alpha^{a^3} \end{aligned}$$

$$\sigma^4(a) = \sigma(\sigma^3(a)) = \sigma(a^3) = a$$

So $\sigma^4 = \text{Id}$

So $\text{Aut}(C_5) \cong C_4$ generated by σ
 $\sigma(a) = a^2$

→ a group
 maybe we can use
 Dabur's group theory
 unpaired 21/01/11

Let C_n cyclic group of order n
 $C_n = \{1, a, \dots, a^{n-1}\}$ $a^n = 1$
 H some group

Q: Describe all homomorphisms
 $\varphi: C_n \rightarrow H$

First observation: $\varphi(a)^n = 1$

Proof: $\varphi(a)^n = \varphi(a^n) = \varphi(1) = 1$ Q.E.D.

Second observation: φ completely determined by value of $\varphi(a)$

Proof: Typical element of C_n is a^r
 $\varphi(a^r) = \varphi(a)^r$

so if you know $\varphi(a)$ then you know $\varphi(a^r)$ Q.E.D.

Prop: Let $n \geq 2$
 $C_n = \{1, a, \dots, a^{n-1}\}$ ($a^n = 1$)
 H group, & let $h \in H$

Then \exists homomorphism $\varphi: C_n \rightarrow H$ with $\varphi(a) = h$
 iff $(\text{ord } h) \mid n$
 $[\text{ord}(h) \mid n]$

Proof

(\Rightarrow) first observation

(\Leftarrow) Suppose $\text{ord}(h)$ div n (so that $h^n = 1$)

Define $\varphi: C_n \rightarrow K$ by $\varphi(a^r) = h^r$

1) This is well defined (proved on 04.04.14 AP)

2) φ is a homomorphism, as:

$$\begin{aligned} \varphi(a^r \cdot a^s) &= \varphi(a^{r+s}) = h^{r+s} \\ &= h^r h^s \end{aligned}$$

$$= \varphi(a^r) \varphi(a^s)$$

Q.E.D

Q: Given $\varphi: C_n \rightarrow K$ as above $\varphi(a) = h$ ($\text{ord}(h)$ div n)
when is φ injective?

A: φ injective $\Leftrightarrow \text{ord}(h) = n$

Proof. (\Leftarrow) Suppose $\text{ord}(h) = n$

look at $\varphi(1), \varphi(a), \dots, \varphi(a^{n-1})$

If φ is not injective, then $\varphi(a^r) = \varphi(a^s)$ for some r, s :
 $0 \leq r < s \leq n-1$

Put $t = s - r$

$$a^s = a^r a^t$$

$$\begin{aligned} \varphi(a^r) \varphi(a^t) &= \varphi(a^s) \\ \varphi(a^r) &= \varphi(a^r) \end{aligned}$$

$\varphi(a^s) = \varphi(a^r) \varphi(a^t)$ then $1 \leq t < n$

Multiply on left by $\varphi(a^r)^{-1}$ to get
 $1 = \varphi(a^t) = \varphi(a)^t$

it is inverse of the element.

so $\text{ord}(\varphi(a)) \leq t < n$ contradiction Q.E.D (\Leftarrow)

(\Rightarrow) If φ injective $(1 = \varphi(1), \varphi(a), \dots, \varphi(a^{n-1}))$ all distinct
 $(1 = \varphi(1), \varphi(a), \varphi(a)^2, \dots, \varphi(a)^{n-1})$ distinct

I know $\varphi(x)^n = \varphi(x^n) = 1$ so

$\text{ord } \varphi(x) \leq n$

If $\text{ord } \varphi(x) = k < n$

so $\text{ord}(\varphi(x)) = n$ QED

contradiction
 $\varphi(x)^k = \varphi(x)$

Q: what do homomorphisms $\varphi: C_n \rightarrow C_n$ look like?

standard def-n.

Let $0 \leq a \leq n-1$

define $\varphi_a: C_n \rightarrow C_n$ by $\varphi_a(x) = x^a$

Previous discussion shows:

Prop-on:

If $\varphi: C_n \rightarrow C_n$ is a homomorphism then $\varphi = \varphi_a$ for some $a: 0 \leq a \leq n-1$

really we would like to know if there are any other homomorphisms? none! no other homomorphisms!

So there are precisely n homomorphisms $\varphi: C_n \rightarrow C_n$

The question which really interests us is

Q: when is φ_a an automorphism $\varphi_a: C_n \xrightarrow{\sim} C_n$?

Prop: $\varphi_a: C_n \rightarrow C_n$ is an automorphism $\Leftrightarrow a$ is coprime to n .

Proof: $\text{ord}(x^a) = \frac{n}{\text{HCF}(a, n)}$

so $\text{ord}(x^a) = n \Leftrightarrow a, n$ coprime
However C_n is finite so

$\varphi: C_n \rightarrow C_n$ is Bijective iff φ is injective
 $\Rightarrow \varphi_a$ is automorphism (it is already homomorphism by above)
 iff φ_a is injective \uparrow (by prop. above)
 iff $\text{ord } a^a = n$
 iff a, n coprime QED

Example 1) Calculate $\text{Aut}(C_7)$

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

There are seven homomorphisms $\varphi: C_7 \rightarrow C_7$

$\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$
 $1, 2, 3, 4, 5, 6$ all coprime to 7

So $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$ all automorphisms

φ_0 is trivial homomorphism: $\varphi_0(a^r) = a^{0r} = 1$
 ($a^r \rightarrow 1$ for $\forall r$, not injective)

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

what is the group structure?

$\varphi_1 = \text{Id}$ (Always!!)

$\varphi_1(x) = x$ $\varphi_1(a^r) = a^r$

Put $\alpha = \varphi_3$

Calculate α^2 :

$\alpha^2(a) = \alpha(\alpha(a)) = \alpha(a^3) = \alpha(a)^3 = (a^3)^3 = a^9 = a^2$

so $\alpha^2 = \varphi_2$

~~Put~~ $\alpha^3(a) = \alpha(\alpha^2(a)) = \alpha(a^2) = \alpha(a)^2 = (a^3)^2 = a^6$

$\alpha^3 = \varphi_6$

$$\alpha^4 : \alpha^4(\alpha) = \alpha(\alpha^4(\alpha)) \\ = \alpha(\alpha^6) = \alpha^8 = \alpha^4$$

$$\alpha^4 = \psi_4$$

$$\alpha^5(\alpha) = \alpha(\alpha^4(\alpha)) = \alpha(\alpha^4) = \alpha^{12} = \alpha^5 \\ \alpha^5 = \psi_5$$

$$\alpha^6(\alpha) = \alpha(\alpha^5(\alpha)) = \alpha(\alpha^5) = \alpha^{15} = \alpha \\ \alpha^6 = \text{Id}$$

$$\text{So } \text{Aut}(C_7) = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\} \\ \begin{matrix} \vdots & \vdots & \vdots & \vdots & \vdots \\ \psi_1 & \psi_2 & \psi_3 & \psi_4 & \psi_5 \end{matrix}$$

Aut(C₉) C₉ = {1, α, ..., α⁸} · α⁹ = 1

$$\text{Aut}(C_9) = \{ \psi_a : a \text{ coprime to } 9 \} \\ = \{ \psi_1, \psi_2, \psi_4, \psi_5, \psi_7, \psi_8 \} \\ \text{Id}$$

Take β = ψ₂

$$\begin{aligned} \beta^2 &= \psi_4 \\ \beta^3 &= \psi_8 \\ \beta^4 &= \psi_7 \\ \beta^5 &= \psi_5 \\ \beta^6 &= 1 \end{aligned}$$

$$\text{Aut}(C_9) \cong C_6 = \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5\} \\ \begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \psi_2 & \psi_4 & \psi_8 & \psi_7 & \psi_5 \end{matrix}$$

3) Aut(C₁₅)

$$C_{15} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\} \quad \alpha^{15} = 1$$

$$\text{Aut}(C_{15}) = \{ \phi_\alpha : \alpha \text{ congruent to } 15 \}$$

$$\{ \phi_1, \phi_2, \phi_4, \phi_7, \phi_8, \phi_{11}, \phi_{13}, \phi_{14} \}$$

$$\phi_1 = \text{Id}$$

$$\text{Put } \alpha = \phi_2$$

$$\alpha^2 = \phi_4 \quad \alpha^2(\alpha) = \alpha(\alpha(\alpha)) = \alpha(\alpha^2) = (\alpha(\alpha))^2 = (\alpha^2)^2 = \alpha^4$$

$$\alpha^3 = \phi_8$$

$$\alpha^4 = \text{Id}$$

$$\text{Put } \phi_2 = \phi_7$$

$$\phi_7^2 = \phi_7(\phi_7(\alpha)) = \phi_4 = \alpha^2 \quad \times \text{ Redundant}$$

$$\text{Put } \gamma = \phi_{11}$$

$$\gamma^2 = \phi_1$$

$$\gamma^2(\alpha) = (\alpha^{11})^{11} = \alpha^{121} = \alpha$$

$$\begin{matrix} \phi_1, \phi_2, \phi_4, \phi_7, \phi_8, \phi_{11}, \phi_{13}, \phi_{14} \\ \text{id}, \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14} \end{matrix}$$

C ₈	x
<u>C₄ × C₂</u>	✓
C ₂ × C ₂ × C ₂	✓
D ₈	x
Q ₈	x

$$(\alpha \gamma)(\alpha) = \alpha(\alpha^{11}) = \alpha^{12} = \alpha^7$$

$$\gamma \alpha(\alpha) = \alpha^7$$

$$(\alpha^{11})^2 = (\alpha^7)^{11}$$

$$(\alpha^2 \gamma)(\alpha) = \alpha^2(\alpha^{11}) = \alpha^{22} = \alpha^{14} = \phi_{14} = \gamma \alpha^2$$

$$\alpha^3 \gamma(\alpha) = \alpha^3(\alpha^{11}) = \alpha^{33} = \phi_{13} = \gamma \alpha^3$$

$$\text{Aut}(C_{15}) = \{1, \alpha, \alpha^2, \alpha^3, \gamma, \alpha \gamma, \alpha^2 \gamma, \alpha^3 \gamma\}$$

$$\alpha^4 = 1 \quad \gamma \alpha = \alpha \gamma$$

$$\gamma^2 = 1$$

$$\text{We showed } \text{Aut}(C_{15}) \cong C_4 \times C_2$$

necessary for max 6 non y elements

Spec Def-n

$$C_n = \{1, a, a^2, a^3\} \quad a^n = 1$$

$$C_2 = \{1, c\} \quad c^2 = 1$$

Formally

$$C_4 \times C_2 = \{(1,1), (a,1), (a^2,1), (a^3,1), (1,c), (a,c), (a^2,c), (a^3,c)\}$$

Trick: $1 \quad A \quad A^2 \quad A^3 \quad C \quad AC \quad A^2C \quad A^3C$

$$AC = CA \quad (a,1)(1,c) = (a,c) \quad A C$$

$$(1,c)(a,1) = (a,c)$$

Beware standard confusion:

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

$$\text{Aut}(C_n) = \{\varphi_a : a \text{ coprime to } n\}$$

$$\varphi_a(x) = x^a \quad \varphi_a \neq x^a$$

Prop $\text{Aut}(C_p) \cong C_{p-1}$ if p is prime

Q/W 3

Revision of last year (not examinable)

Def-n let G be a group and $H \subseteq G$

Say that H is a subgroup of G , when

- (i) $\forall x, y \in H \quad xy \in H$
- (ii) $1 \in H$
- (iii) $\forall x \in H \quad x^{-1} \in H$

equivalently when

- (a) $x \in H$
- (b) $\forall x, y \in H, xy^{-1} \in H$

Lagrange Theorem

Lagrange's Theorem

If H is a subgroup of the finite group G then $|H|$ divides $|G|$ exactly

Proof I

Def-n let 1) G be a group and
2) $H \subset G$ a subgroup
If $x \in G$ $xH = \{xh : h \in H\}$ left coset of H by x
 $Hx = \{hx : h \in H\}$ Right coset

Example: $G = D_3 = \{1, a, a^2, y, ay, a^2y\}$ $a^3 = 1$ $ya = a^2y$
 $y^2 = 1$

Take $H = \{1, y\}$ is a subgroup

Left cosets

- $1 \cdot H = \{1 \cdot 1, 1 \cdot y\} = \{1, y\} = H$
- $aH = \{a \cdot 1, a \cdot y\} = \{a, ay\}$
- $a^2H = \{a^2 \cdot 1, a^2 \cdot y\} = \{a^2, a^2y\}$
- $yH = \{y \cdot 1, y \cdot y\} = \{y, 1\} = H$
- $ayH = \{ay \cdot 1, ay \cdot y\} = \{ay, a\}$
- $a^2yH = \{a^2y \cdot 1, a^2y \cdot y\} = \{a^2y, a^2\}$

Right cosets

- $H \cdot 1 = \{1, y\} = H$
- $H \cdot a = \{a, ya\} = \{a, a^2y\}$
- $H \cdot a^2 = \{a^2, ya^2\} = \{a^2, ay\}$
- $H \cdot y = \{y, 1\} = H$
- $H \cdot ay = \{ay, a^2\} = H \cdot a^2$
- $H \cdot a^2y = \{a^2y, y\} = H \cdot a$

Note: $aH \neq Ha$, usually (when G is not abelian gr.)

25.01.11

II

Prop
There exists a bijective mapping
 $H \leftrightarrow xH$ (true for any $x \in G$)

Proof:

Part $\gamma: K \rightarrow \alpha K \quad \gamma(h) = \alpha h$

γ injective $\gamma(h_1) = \gamma(h_2)$
 $\alpha h_1 = \alpha h_2$
 $\alpha^{-1} \alpha h_1 = \alpha^{-1} \alpha h_2$
 $h_1 = h_2$

γ is surjective by defⁿ of αK **QED**

III Corollary $\forall \alpha \in G \quad |\alpha K| = |K|$

Example $G = D_4 = \{1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma\}$
 $K = \{1, \gamma\}$

$1 \cdot K = \gamma K = \{1, \gamma\}$
 $\alpha \cdot K = \alpha\gamma K = \{\alpha, \alpha\gamma\}$
 $\alpha^2 \cdot K = \alpha^2\gamma K = \{\alpha^2, \alpha^2\gamma\}$

Observe distinct cosets are disjoint
 True in general!

IV Prop.

Let $a, b \in G$
 then either $aK = bK$
 or $aK \cap bK = \emptyset$

Proof

need to proof: $aK = bK \Leftrightarrow aK \cap bK \neq \emptyset$
(\Rightarrow) $aK = bK \rightarrow aK \cap bK \neq \emptyset$ (by logic)

S.p.

It suffices to show that if $(aK \cap bK) \neq \emptyset$ then $aK = bK$

So suppose $z \in (aK) \cap (bK)$

so $z = ah_1$ for some $h_1 \in K$
 $z = bh_2$ for some $h_2 \in K$

so $ah_1 = bh_2$
 $b^{-1}a = h_2 h_1^{-1} \in K$
 $a = b b^{-1} a = b h_2 h_1^{-1} \in bK$

so for each $y \in K$
 $ay = b h_2 h_1^{-1} y \in bK$

i.e. if $(aK) \cap (bK) \neq \emptyset$
then $aK \subset bK$

so by

Repeat the argument using the fact $(bK) \cap (aK) \neq \emptyset$
to get $bK \subset aK$

so if $(aK) \cap (bK) \neq \emptyset$
 \square then $aK = bK$ Q.E.D.

Main Pr: Coset Lagrange's Theorem

If G is a finite group and K
 $\Rightarrow K \subset G$ is a subgroup

Then $|K|$ divides $|G|$ exactly

Proof: list different (ie distinct) cosets x_1, \dots, x_m

each X_i has the form
 $X_i = x_i K$ for some $x_i \in G$

claim: $G = \bigcup_{i=1}^m X_i$

because of $g \in G$, then $g \in gK$ and $gK = X_r$
 for some r .

so $g \in \bigcup_{r=1}^m X_r$ for $\forall g \in G$

But distinct cosets are disjoint
 i.e. $X_i \cap X_j = \emptyset$ if $i \neq j$

so $|G| = |X_1| + |X_2| + \dots + |X_m|$
 $|G| = |x_1 K| + |x_2 K| + \dots + |x_m K|$

But $|x_i K| = |K|$ for each i , so

$|G| = m|K|$ QED.

$m =$ num. of distinct cosets □

In the proof I've listed the distinct cosets in the form: $a_1 K, a_2 K, \dots, a_m K$

$a_i K \cap a_j K = \emptyset$ if $i \neq j$

$\{a_1, \dots, a_m\}$ is then called a set of **coset representatives**.
 There is no uniqueness about $\{a_1, \dots, a_m\}$

Example $G = D_6 = \{1, r, r^2, y, ry, r^2y\}$
 $H = \{1, y\}$

The distinct cosets are

$1 \cdot H, r \cdot H, r^2 \cdot H$
 so $\{1, r, r^2\}$ is a set of coset reps for H on G

$y \cdot H, ry \cdot H, r^2y \cdot H$ also list the distinct cosets
 $\begin{matrix} yH & ryH & r^2yH \\ \parallel & \parallel & \parallel \\ H & rH & r^2H \end{matrix}$

so $\{y, ry, r^2y\}$ is also a set of coset reps

$\{y, r, r^2\}$

Q: When is $aK = bK$?

A: $aK = bK \Leftrightarrow b^{-1}a \in H$ Rule of equality of left cosets

Prop Rule of equality
 $aK = bK \Leftrightarrow b^{-1}a \in K$

Proof: Suppose $aK = bK$

For some $h_1, h_2 \in K$ $a h_1 = b h_2$
 so $b^{-1}a = h_2 h_1^{-1} \in H$ (QED \Rightarrow)

\Leftarrow) Suppose $b^{-1}a \in H$

so $a = b h$ for some $h \in K$
 so $a h' = b h h'$ for all $h' \in H$
 $\begin{matrix} a h' \\ b h \end{matrix}$

so $aK \subset bK$

But $(b^{-1}a)^{-1} \in K$ (K subgroup)

$a^{-1}b \in V$

so by symmetry $bK \subset aK$

$\therefore b^{-1}a \in K \Rightarrow aK = bK$ Q.E.D.

Investigation: semidirect product

2/1/11: 28.01.11

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

$x^3 = 1$

$y^2 = 1$

$yx = x^2y$

Contrast this with $C_3 \times C_2$

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

$C_2 = \{1, y\}$

$x^3 = 1, y^2 = 1$

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

$\begin{matrix} \text{"} & \text{"} & \text{"} & \text{"} & \text{"} & \text{"} \\ 1 & x & x^2 & y & xy & x^2y \end{matrix}$

Jan Austen says that $D_6 = C_3 \times C_2$

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

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

but is wrong!

$D_6 \quad x^3 = 1 \quad y^2 = 1 \quad yx = x^2y (\neq xy)$

$\hookrightarrow C_3 \times C_2 \quad x^3 = 1 \quad y^2 = 1 \quad yx = xy$

→ consequence of conjugation

Semidirect Products

Suppose G is a group $g \in G$

Consider $\sigma_g: G \rightarrow G$ defined by $\sigma_g(a) = g^{-1}ag$

Prop

ig is an automorphism of G

B Proof: 1) ig is homomorphism:

$$ig(xy) = g(xy)g^{-1} = g \cdot x \cdot g^{-1} \cdot g \cdot y \cdot g^{-1} = ig(x)ig(y)$$

2) ig is invertible with inverse $(ig)^{-1} = ig^{-1}$

$$\begin{aligned} (ig^{-1}ig)(x) &= ig^{-1}(g \cdot x \cdot g^{-1}) \\ &= g^{-1} \cdot g \cdot x \cdot g^{-1} \cdot g \\ &= g^{-1} \cdot g \cdot x \cdot (g^{-1}g) \\ &= x \end{aligned}$$

workings
idea
max before
output with
new.

$E \quad ig^{-1}ig = Id \quad igig^{-1} = id \quad Q.E.D$

look at the assignment

$$\begin{array}{ccc} \hookrightarrow g & \hookrightarrow & ig \\ i: G & \longrightarrow & \text{Aut}(G) \end{array}$$

Prop:

$i: G \rightarrow \text{Aut } G$ is a homomorphism

B Proof: $ig(h(a)) = g(h(a))(g^{-1})^{-1}$
and $(gh)^{-1} = h^{-1}g^{-1}$

so $ig(h(a)) = g(h \cdot a \cdot h^{-1})g^{-1} = ig(h \cdot a \cdot h^{-1}) = ig(i_h(a)) = ig \circ i_h(a)$

(Note: Mult in $\text{Aut } G$ is by composition)

E True for all a so $ig \circ h = ig \circ i_h \quad Q.E.D$

Go back and look at D_6
 $D_6 = \{1, x, x^2, y, xy, x^2y\}$

Take $K = \{1, x, x^2\}$ subgp of D_6
 $Q = \{1, y\}$ " " D_6

look at homomorphism

$$i: Q \rightarrow \text{Aut}(D_6)$$

$$i(\text{id } g) = 1g1^{-1} = \text{id}$$

$$i(y) = ygy^{-1}$$

$i_1 = 1$
 , where $g \in g$

$$i(y)(1) = y1y^{-1} = 1$$

$$i(y)(x) = yxy^{-1} = x^2yy^{-1} = x^2$$

$$i(y)(x^2) = yx^2y^{-1} = xy^2y^{-1} = x$$

Notice in this case: i_y defines an automorphism of K

Write $K = \{1, x, x^2\}$
 $Q = \{1, y\}$

Define a new multiplication on $K \times Q$, in order to produce D_6 rather than $C_3 \times C_2$

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

I want $yx = x^2y$ to get D_6
 what do I need to do?

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

$$= (i_y(x), y)$$

good motivation in your answer so keep standard

theory in definition = system in bee
where there not more groups than homomorphisms?

Semidirect products:

- Three ingredients:
- 1) a group K
 - 2) a group Q
 - 3) a homomorphism

$\varphi: Q \rightarrow \text{Aut}(K)$ (operator homomorphism)

New multiplication Rule

$*$: $(K \times Q) \times (K \times Q) \rightarrow K \times Q$
 $(k_1, q_1) * (k_2, q_2) = (k_1 \varphi(q_1)(k_2), q_1 q_2)$

Sp/w: have to check this gives a group (Exercise)

Four cases: $(k_1, 1) * (k_2, 1) = (k_1 \varphi(1)(k_2), 1 \cdot 1)$
 $\varphi: Q \rightarrow \text{Aut}(K)$ $\varphi(1)(k_2) = k_2$ $\varphi(1) = \text{Id}$

I $(k_1, 1) * (k_2, 1) = (k_1 k_2, 1 \cdot 1) = (k_1 k_2, 1)$ no surprise!

II $(k, 1) * (1, q) = (k \varphi(1)(1), 1 \cdot q) = (k, q)$ no surprise!

III $(1, q_1) * (1, q_2) = (1 \varphi(q_1)(1), q_1 q_2) = (1, q_1 q_2)$
 $\varphi(q_1) \in \text{Aut } K$ so $\varphi(q_1)(1) = 1$ no surprise!

IV CRUCIAL CASE:

$(1, q) * (k, 1) = (1 \varphi(q)(k), q \cdot 1) = (\varphi(q)(k), q)$

So $(1, q) * (k, 1) = (\varphi(q)(k), q)$

All other cases are derived from these 4 main cases (see notes for details)

D_6 compared with $C_3 \times C_2$

$$K = C_3 = \{1, a, a^2\} \quad a^3 = 1$$

$$Q = C_2 = \{1, y\} \quad y^2 = 1$$

Final ingredient is a homomorphism

$$\varphi: Q \rightarrow \text{Aut } K$$

$$\varphi: C_2 \rightarrow \text{Aut}(C_3)$$

$$\text{Aut}(C_3) \cong C_2 = \{1, \tau\} \quad \tau(a) = a^2, \tau(a^2) = a$$

Q: How many homomorphism $C_2 \xrightarrow{h} \text{Aut}(C_3)$?

A: Two:

- 1) $h(y) = 1$ trivial
 - 2) $h(y) = \tau$ non-trivial
- } \Rightarrow

Calculate product in non-trivial case

$$(1, y) * (x, 1) = (h(y)(x), y)$$

$$= (\tau(x), y)$$

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

$$y * x = x^2 y$$

I've got D_6

as was in trivial case

$$(1, y) * (x, 1) = (h(y)(x), y) \quad \text{as } h(y) = 1$$

$$= (x, y) \quad h(y)(x) = x$$

{End} $y * x = xy \quad C_3 \times C_2$

non-trivial homomorphism

Def-n 'Formal'

Let K be a group
 Q be a group
 $h: Q \rightarrow \text{Aut}(K)$ a homomorphism

then the **semidirect product**

$K \rtimes_h Q$

is obtained as follows

- 1) Underlying set is $K \times Q$
- 2) multiplication: $*$ $(K \times Q) \times (K \times Q) \rightarrow K \times Q$ given by
 $(k_1, q_1) * (k_2, q_2) = (k_1, h(q_1)(k_2), q_1 q_2)$

The nonabelian group of order 21, $G(21)$
 $K \rtimes_h Q$ $h: Q \rightarrow \text{Aut}(K)$

1/02/11

Here we take $K = C_7 = \{1, x, x^2, x^3, x^4, x^5, x^6\}$ $x^7 = 1$
 $Q = C_3 = \{1, y, y^2\}$ $y^3 = 1$

We need a homomorphism $h: C_3 \rightarrow \text{Aut}(C_7)$

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

41
27
189
54
129

φ_3 has order 6 \rightarrow underlying

φ_3	$= \varphi_3$	x	6	\leftarrow
φ_3^2	$= \varphi_2$	x^2	3	\leftarrow
φ_3^3	$= \text{Id}$	x^3	2	\leftarrow
φ_3^4	$= \varphi_4$	x^4	3	\leftarrow
φ_3^5	$= \varphi_5$	x^5	6	
φ_3^6	$= \text{Id}$	x^6	1	\leftarrow

$\varphi_3(x) = x^2$
 $\varphi_3^2(x) = \varphi_3(\varphi_3(x)) = \varphi_3(x^2) = x^4 = x^2 \cdot x^2 = x^4$

$\varphi_3(x^2) = \varphi_3(x) \varphi_3(x) = x^2 \cdot x^2 = x^4$

$\varphi_3^3(x) = \varphi_3(\varphi_3^2(x)) = \varphi_3(x^4) = x^8 = x = \text{Id}$
 $\varphi_3(x^3) = \varphi_3(x) \varphi_3(x) \varphi_3(x) = x^2 \cdot x^2 \cdot x^2 = x^6 = x^{-1}$

$\varphi_3^6(x) = (x^2)^2 \cdot (x^2)^2 \cdot (x^2)^2 = x^6 = x^{-1} = x^6 = \text{Id}$

Must have odd ky Div. 3

Three possible homomorphisms:

1) Trivial choice $h(y) = Id$

- 2) 1st non trivial choice $h(y) = \rho_2$ $h(y) = \rho_2(a) = a^2$
 3) 2nd non trivial choice $h(y) = \rho_4$

① with 1st non-trivial choice
 crucial calculation

$$(1, y) * (a, 1) = (h(y)(a), y)$$

$$\text{so } (1, y) * (a, 1) = (a^2, y)$$

Write $X = (a, 1)$ $Y = (1, y)$

$$\text{so } X^7 = 1 \quad Y^3 = 1$$

crucial calculation: $YX = X^2Y$

So get a group of order 21 whose elements are

- | | |
|---|-------------|
| $1, X, X^2, X^3, X^4, X^5, X^6$ | } Canonical |
| $Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y$ | |
| $Y^2, XY^2, X^2Y^2, X^3Y^2, X^4Y^2, X^5Y^2, X^6Y^2$ | |

The multiplication on this group is given by

$$X^7 = 1, \quad Y^3 = 1, \quad YX = X^2Y$$

② Next take the trivial choice
 $h(y) = Id$ $h(x) = x$

Critical calculation becomes

$$(1, y) * (x, 1) = (h(y)(x), y)$$

$$(1, y) * (x, 1) = (x, y) = (x, 1) * (1, y)$$

So $yx = xy$ *

$x^7 = 1$ $y^3 = 1$ $C_7 \times C_3$

So trivial case gives Direct product

Prop. Trivial choice always gives Direct Product

③ Now let's take 2nd non trivial choice
 $h(y) = \psi_4$ $\varphi_n(x) = x^4$

Critical case: $(1, y) * (x, 1) = (x^4, y)$
 $yx = x^4y$, $x^7 = 1$, $y^3 = 1$

Conclusion:

- For each choice I get a group of order 21 whose elements have canonical form $x^a y^b$ ($0 \leq a \leq 6$, $0 \leq b \leq 2$)

0	Trivial choice	$x^7 = 1$ $y^3 = 1$	$yx = xy$
I	1 st non-triv. ch.	$x^7 = 1$ $y^3 = 1$	$yx = x^2y$
II	2 nd non-triv. ch.	$x^7 = 1$ $y^3 = 1$	$yx = x^4y$

How many different groups?

At least 2 (one commutes, one doesn't)

At most 3

In fact (I) \cong (II)

start with 2nd non-triv. ch. again

$$h: C_3 \rightarrow \text{Aut}(C_3)$$

$$1 \rightarrow 1$$

$$y \rightarrow \psi_1 \quad (\psi_1)^2 = \psi_2$$

$$y^2 \rightarrow \psi_2$$

Put $z = y^2 \in C_3$ $z^2 = y$

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

$$h: C_3 \rightarrow \text{Aut}(C_3)$$

$$1 \rightarrow 1$$

$$z \rightarrow \psi_2$$

$$z^2 \rightarrow \psi_1$$

So now $(1, z)(x, 1) = (z^2, z)$

$$zx = x^2z$$

$$x^3 = 1 \quad z^3 = 1 \quad zx = x^2z$$

(I) \cong (II) by taking change of variables $y \rightarrow y^2$ in C_3

Eventually we'll see that these are the only groups of order 21:

$C_{21} \cong C_7 \times C_3$ Abelian

$G(21) = \langle xy \mid x^7 = 1, y^3 = 1, yx = x^2y \rangle$ non-abelian

Example $C_{11} \rtimes C_5$ $C_5 \rightarrow \text{Aut}(C_{11})$
 $\{1, y, \dots, y^4\}$

$\text{Aut}(C_{11}) \cong C_{10} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9\}$ $2 = \varphi_2$
~~order~~ $\alpha \rightarrow \varphi_2$
 orders $1, 10, 5, 10, 5, 2, 5, 10, 5, 10$

So get 5 homomorphisms
 $h_0, \dots, h_4 : C_5 \rightarrow \text{Aut}(C_{11})$
 $h_0(y) = 1$
 $h_1(y) = \varphi_4 \rightarrow yx = x^4y$
 $h_2(y) = \dots$
 $h_3(y) = \dots$
 $h_4(y) = \dots$

W/W 5 Most groups of "small order" are semidirect products
 ("small" = divisible by two primes a small number of times)
 e.g. 14×43 small, 16 big)

we need a method of recognising when we have a semidirect product

Recognition criteria

Def - Normal subgroups

Suppose K is a subgroup of G
 say that K is normal in G
 when $\forall a \in G \quad aK = Ka$

Equivalently,
 K is normal in G , when $\forall x \in G \forall k \in K \quad xkx^{-1} \in K$

French: "distingué"

example $|G| = D_8 \quad K = \{1, \alpha, \alpha^2\}$

K is normal in D_8 , as

$\alpha k = k \alpha$

as $k = \alpha k = \alpha^2 k \quad || \quad \text{so } \alpha k = k \alpha$
 $k = k \alpha = k \alpha^2 \quad || \quad \alpha^2 k = k \alpha^2$

$yK = \{y, y\alpha, y\alpha^2\} = Ky$
 $= \{y, \alpha y, \alpha^2 y\}$

$yK = Ky$
 $\alpha yK = K\alpha y$
 $\alpha^2 yK = K\alpha^2 y \quad \Rightarrow \text{QED}$

whereas in D_8 if $K = \{1, \alpha\}$
 $\alpha k = \{\alpha, \alpha^2\} \quad K\alpha = \{\alpha, \alpha^2\}$
 $\alpha k \neq K\alpha$ so K not normal

If K is normal in G with
 $K \triangleleft G$

Then Recognition Criterion:

- Let G be a finite group
 Suppose G has subgroups K, Q , s.t.
- i) $K \triangleleft G$
 - ii) $|G| = |K||Q|$
 - iii) $K \cap Q = \{1\}$
- then $G \cong K \rtimes Q$ for some homomorphism $\iota: Q \rightarrow \text{Aut}(K)$

e.g. in $D_3 = G$

$$K = \{1, a, a^2\} \quad |K| = 3$$

$$Q = \{1, b\} \quad |Q| = 2$$

$$K \triangleleft G \quad K \cap Q = \{1\} \quad |G| = |K| |Q|$$

$$\text{so } D_3 \cong K \rtimes Q \quad (= C_3 \rtimes C_2)$$

Proof of Recogn. Criterion

Suppose given G, K, Q as above
let $q \in Q, k \in K$

Because $K \triangleleft G$ I know $q k q^{-1} \in K$

$$(q k q^{-1} \in K)$$

$$(q k = k q)$$

Define $h: Q \rightarrow \text{Aut}(K)$ by

$$h(q)(k) = q k q^{-1}$$

Each $h(q)$ is truly an automorphism of K :

$$h(q)(k_1 k_2) = q k_1 k_2 q^{-1} \quad \left| \quad h_q(a) = q a q^{-1} \right.$$

$$= (q k_1 q^{-1}) (q k_2 q^{-1}) \quad \left| \quad h_q(k_1 k_2) = h_q(k_1) h_q(k_2) \right.$$

$$= h(q)(k_1) h(q)(k_2)$$

QED

Note $\exists h(q)^{-1} = h(q^{-1}) \Rightarrow h(q)$ is bijective

h is itself a homomorphism:

$$h(q_1 q_2) k = q_1 q_2 k (q_1 q_2)^{-1}$$

$$= q_1 [q_2 k q_2^{-1}] q_1^{-1} = h(q_1) [q_2 k q_2^{-1}] = h(q_1) \circ h(q_2)(k)$$

$$\text{so } h(q_1 q_2) = h(q_1) \circ h(q_2)$$

claim: that $g \cong K \triangleleft_h g$ ($= K \times Q$ w/ multiplication by h)
(\Leftrightarrow)

Define $\Phi: K \times_h Q \rightarrow g$ by

$$\Phi(k, q) = kq$$

claim that Φ is a bijective homomorphism (i.e. an \cong)

1) Φ is a homomorphism:

$$\begin{aligned} \Phi((k_1, q_1) * (k_2, q_2)) &= \Phi(k_1 h(q_1) k_2, q_1 q_2) = k_1 h(q_1) k_2 q_1 q_2 \\ &= k_1 k_2 q_1 q_2 = k_1 q_1 k_2 q_2 = \Phi(k_1, q_1) \Phi(k_2, q_2) \end{aligned}$$

So Φ is a homomorphism, as claimed

2) Φ is injective:

$$\begin{aligned} \text{Suppose } \Phi(k, q) &= \Phi(k', q') \\ \therefore kq &= k'q' \\ (k')^{-1}k &= q'q^{-1} \end{aligned}$$

But $(k')^{-1}k \in K$ and $q'q^{-1} \in Q$

$$\text{so } (k')^{-1}k \in K \cap Q = \{1\}$$

$$\text{so } (k')^{-1}k = 1 \quad \text{so } k = k'$$

Similarly $q = q'$.

$$\text{so } \Phi(k, q) = \Phi(k', q') \Rightarrow k = k' \text{ and } q = q'$$

i.e. Φ injective

$$|K \times Q|$$

by hypothesis

But $|K \times \{0\}| = |K| |Q| = |G|$

$\Phi: K \times \{0\} \rightarrow G$ injective both finite sets same size $\implies \Phi$ is surjective QED.

Classification of groups:

obvious statement:

If p is prime and $|G| = p$ then $G \cong C_p$

Proof

let $x \in G$ $|G| \neq 1$

order) Div. $|G|$ $ord(x) \neq 1$

so $ord(x) = p$

and (by listing):

$$G = \{1, x, x^2, \dots, x^{p-1}\} \quad x^p = 1$$

so $G \cong C_p$ \blacksquare

we'll show

Proof If $|G| = 2p$ $p \nmid prime$
then either $G \cong C_{2p}$
or $G \cong D_{2p}$

Proof

let $|G| = 2p$

Suppose I know (by some method or other)

- that
- (1) G has an element x of order p ($ord(x) = p$)
 - (2) $G \dots \dots \dots y \dots \dots \dots z$ ($ord(y) = 2$)

If I knew this, then

if 1) $\exists x \in G$ s.t. $ord x = p$
 and 2) $\exists y \in G$ s.t. $ord y = 2$
 \Rightarrow 3) $|G| = 2p$

Prop. $G \cong C_p \rtimes_h C_2$ for some $h: C_2 \rightarrow \text{Aut}(C_p)$
 p odd prime

Proof:

Write $K = \{1, x, \dots, x^{p-1}\} \cong C_p$ ($ord(x) = p$)

$Q = \{1, y\} \cong C_2$ ($ord(y) = 2$) \rightarrow for i $\exists y^i \in K$ and some $u \in \langle y \rangle$ such that $y^i = x^u$

$|K||Q| = |G| = 2p$ $p \times 2$ i.e. $y = x^i$

$y \notin K$ as $ord(y) = 2 \neq p$ (not div)

so $K \cap Q = \{1\}$

Also K is normal in G

$G/K \cong \langle K, yK \rangle$ $G = K \cup yK$ $K \cap yK = \emptyset$
 $K \cong \langle K, ky \rangle$ $G = K \cup ky$ $K \cap ky = \emptyset$ \Rightarrow

\Rightarrow so $ky = yk$

so $a^p y^b k = k a^p y^b$ ($\forall a, b$)

i.e. K is normal.

So conditions for Recognition criterion hold

so $G \cong K \rtimes_h Q$
 $\cong C_p \rtimes_h C_2$ for some h \blacksquare

So to complete the classification of groups of order $2p$ we need to know:

1) G has an element of order p

necessary condition

G/K

- 2) G has element of order 2
- 3) Describe all homomorphisms $h: G \rightarrow \text{Aut}(C_2)$

First show
Theorem

Let G be a finite group
 Suppose that $\forall g \in G, g^2 = 1$
 Then $G \cong \underbrace{C_2 \times C_2 \times \dots \times C_2}_n$

In partic. $|G| = 2^n$

Proof:

G is necessary abelian:

let $x, y \in G$ $x^2 = 1$ $y^2 = 1$ | $x^{-1} = x$
 also $(xy)^2 = 1$ | $y^{-1} = y$

$xyxy = 1$
 $(xy)^{-1} = xy$ \parallel \Rightarrow $ya = ay$ for all x, y
 $y^{-1}x^{-1} = xy$

Next rewrite G additively:

1 becomes 0
 $x^2 = 1 \dots \Rightarrow 2x = 0$

isomorphic
reminiscent

so G is a vector space over $\mathbb{F}_2 = \{0, 1\}$ (field with 2 elements)

so $G \cong \underbrace{\mathbb{F}_2 \oplus \dots \oplus \mathbb{F}_2}_n$

$\dim G = n$ $|G| = 2^n$

View of G multiplicatively again

$$G \cong C_2 \times C_2 \times \dots \times C_2$$

$$\mathbb{F}_2 = \{0, 1\} \cong C_2 = \{1, x\}$$

$$0 \rightarrow 1$$

$$1 \rightarrow x$$

Q.E.D.

08/02/11
We showed that if g satisfies $x^2=1$ for all $x \in g$
then $|g| = 2^n$ ($g \cong \underbrace{C_2 \times C_2 \times \dots \times C_2}_n$)

let p be odd prime and

$$|g| = 2p$$

(we'll show $g \cong C_{2p}$ & $g \cong D_{2p}$)

let $x \in g$

$$\text{ord}(x) \text{ divides } |g| = 2p$$

$$\text{either } \text{ord}(x) = 1 \quad (x=1)$$

$$\text{or } \text{ord}(x) = 2$$

$$\text{ord}(x) = p$$

$$\text{ord}(x) = 2p$$

It can't be true that every $x \in g$ satisfies $x^2=1$
otherwise $|g| = 2^n$ whereas $|g| = 2p$ (p -odd)

So either

$$\text{i) } \exists x \in g : \text{ord}(x) = p \quad \text{or}$$

$$\text{or ii) } \exists x \in g : \text{ord}(x) = 2p$$

Prop. let p be an odd prime, and
 G group $|G| = 2p$
 then a) $\exists x \in G$ ord $x = p$
 b) $\exists y \in G$ ord $y = 2$

Proof:
 suppose (i) above holds
 let $z \in G$ have ord $(z) = 2p$
 then $x = z^2$ ord $x = p$
 & $y = z^p$ ord $y = 2$

If (i) above holds no problem about a), but still need to establish b)

So suppose (i) above holds & $z \in G$ have ord $(z) = 2p$
 let $x \in G = \text{ord}(x) = p$
 why it is a subgroup? $K = \{1, x, \dots, x^{p-1}\}$ K is a subgroup of G
 how do we know that K is a subgroup? K is a subgroup of G
 consider $G/K = |G/K| = |G|/|K| = 2p/p = 2$ why this?

So $G = K \cup wK$ for some $w \notin K$

then $w^2 \in K$. If not get
 $w^2K = wK$ only 2 cosets
 so $wK = K$ (multiply by w^{-1})
 which would imply $w \in K$ (contradiction)

As $\omega^2 \in K$ either

$$\omega^2 = 1 \quad \text{or} \quad \omega^2 = \alpha^q \quad (1 \leq q \leq p-1)$$

If $\omega^2 = 1$ put $y = \omega \Rightarrow \text{ord}(y) = 2$

If $\omega^2 \neq 1$ then $\text{ord}(\omega^2) = p \rightarrow$ any 2 disagree

so $\text{ord}(\omega) = 2p$ and put $y = \omega^p \Rightarrow \text{ord}(y) = 2$

This exhausts all possibilities

In any case $\exists x \in G \text{ ord}(x) = p$
 $\exists y \in G \text{ ord}(y) = 2$ □

{The story so far...

$$|G| = 2p \quad \exists x \in G \text{ ord}(x) = p$$

$$\exists y \in G \text{ ord}(y) = 2$$

Now read on!

Theorem: Let p be an odd prime and $|G| = 2p$
 then $G \cong C_p \rtimes_h C_2$ for some $h: C_2 \rightarrow \text{Aut}(C_p)$

Proof: (already in details proved by parts: look previous them)

extra work:

$$K = \{1, \alpha, \dots, \alpha^{p-1}\} \quad \alpha^p = 1 \quad \text{ord}(\alpha) = p$$

$$Q = \{1, y\} \quad y^2 = 1 \quad \text{ord}(y) = 2$$

$$K \cong C_p \quad Q \cong C_2$$

claim that $K \triangleleft Q$ why?

$$G = K \cup yK \quad (y \notin K)$$

$$G = K \cup Ky \quad \text{so } yK = Ky \quad (\text{only } = \text{cosets})$$

$$x^2 K = K x^2 \quad (x^a \in K)$$

$$\text{so } x^a y^b K = K x^a y^b \quad 0 \leq a \leq p-1$$

$$\text{so } K \triangleleft Q \text{ as claimed} \quad 0 \leq b \leq 1$$

Now apply Recognition criterion

$$[|G| = |K| |Q| \quad (2p = p \times 2)]$$

$$\text{So } G \cong K \rtimes_{\alpha} Q$$

$$\cong C_p \rtimes_{\alpha} C_2 \quad \text{for some } \alpha: C_2 \rightarrow \text{Aut}(C_p)$$

How many homomorphisms $\alpha: C_2 \rightarrow \text{Aut}(C_p)$?

Trick: let $\alpha: C_p \rightarrow C_p$ (p -prime)
be an automorphism satisfying $\alpha^2 = \text{id}$
then either $\alpha = \text{id}$ or $\alpha(x) = x^{-1}$

Proof: let $C_p = \{1, \alpha, \dots, \alpha^{p-1}\}$ & consider $\alpha \alpha(x) \in C_p$
Either (a) $\alpha \alpha(x) = 1$ or (b) $\alpha \alpha(x) \neq 1$

if (a) $\alpha \alpha(x) = 1$
(b) then $\alpha \alpha(x)$ generates C_p i.e. $\alpha \alpha(g) = 1$ or $= \alpha$
as $\alpha \alpha(x) \neq 1 \in C_p$ & $\forall g \in C_p$ ord(g) | p
 $= \alpha(\alpha \alpha(x)) = \alpha$

$$\text{but } \alpha(\alpha \alpha(x)) = \alpha \alpha^2(x)$$

$$= \alpha \alpha(x) \alpha$$

$$= \alpha \alpha(x) \quad (C_p \text{ abelian})$$

σ does twice a generator to itself, so $\sigma = \text{id}$

Corollary: If P is an odd prime & $|G| = 2P$
 Then either $G \cong C_{2P} (\cong C_P \times C_2)$
 or $G \cong D_{2P}$

Proof: Let $G \cong C_P \rtimes_h C_2$
 where $h: C_2 \rightarrow \text{Aut}(C_P)$

let $C_P = \{1, \sigma, \dots, \sigma^{P-1}\}$ & $C_2 = \{1, \tau\}$

look at $h(\tau) \in \text{Aut}(C_P)$ (& h is homomorphism)

clearly $h(\tau)^2 = \text{id} (= h(\tau^2))$

so either $h(\tau) = \text{id}$ & $G \cong C_P \times C_2 \cong C_{2P}$
 or $h(\tau)(\sigma) = \sigma^{-1}$ & $G \cong D_{2P}$

any odd order group

how far have we got?

order	groups	complete
1	1	✓
2	C_2	✓
3	C_3	✓
4	$C_4, C_2 \times C_2$?
5	C_5	✓
6	C_6, D_6	✓
7	C_7	✓

order	Groups	complete
8	$C_8, C_4 \times C_2, C_2 \times C_2 \vee C_2,$	D_8, Q_8 ?
9	$C_9, C_3 \times C_3$?
10	C_{10}, D_{10}	✓
11	C_{11}	✓
12		✓
13	C_{13}	✓
14	C_{14}, D_{14}	✓
15	C_{15}	✓
16	Men	✓
17	C_{17}	✓
18		✓
19	C_{19}	✓
20		✓
21	$C_{21}, G(21)$?
22	C_{22}, D_{22}	✓

11/02/11

last lecture:

p odd prime
 $|G| = 2p$ then $G \cong C_{2p}$ or $G \cong D_{2p}$

isomorphism

If $p=2$ $2p=4$
 $|G|=4$ then either $G \cong C_4$ or $G \cong C_2 \times C_2$ ($\neq D_4$)

Proof:

if $\exists a \in G$
 $\text{ord}(a) = 4$ then $G \cong C_4$
 the alternative

non-cyclic group? yes

$\exists x \in G: x^2 = 1$ we've then $G \cong C_2 \times C_2$ QED

We need to show:

- (i) G has an element of order p
- (ii) G " " " " " " 2

We come to

then Sylow's Theorem (= 'real stuff')

let p be a prime
 G be a finite group s.t. $|G| = k p^n$,
 where k is coprime to p

- then
- (i) G has a subgroup of order p^n
 - (ii) if $N_p = \text{num. of subgroups of order } p^n$
 then $N_p \equiv 1 \pmod{p}$
 - (iii) $N_p \text{ divides } |G|$
 - (iv) If H is a subgroup of order p^m ($m \leq n$),
 and K is a subgroup of order p^n ,
 then $\exists x \in G$ s.t. $x K x^{-1} \subset K$

Example of "Sylow counting"

we show that if $|G| = 21$

then either $G \cong C_{21} \cong C_3 \times C_7$

or $G \cong G(21)$ (non-abelian of order 21)

$|G| = 21 = 7 \times 3$

tip: go for the biggest prime first

$$|G| = kp^n \quad (k=3, p=7, n=1)$$

By Sylow's \exists subgroup of K with $|K| = 7$
i.e. $K \cong C_7$

N_7 = the number of such subgroup

Sylow's (ii) tells us that either $N_7 = 1$
or $N_7 \geq 8$

claim that, in fact, $N_7 = 1$

otherwise suppose $N_7 \geq 8$

let K_1, \dots, K_8 each be a subgroup of order 7

each K_i has 6 elements of order 7

recall: $\text{ord}(x) \mid |K|, i.e. = 1 \text{ or } 7$

Also $K_i \cap K_j = \{1\}$ if $i \neq j$ \rightarrow necessary?

(non trivial element in $K_i \cap K_j$ generates both K_i & K_j
 $\implies K_i = K_j$)

so I have at best $8 \times (7-1) = 48$ elements of order 7

However $|G| = 21 < 48$

contradiction:

Hence $N_7 = 1 \implies K$ is unique

So let K be the unique subgroup of order 7
if $x \in G$ $x^7 \in K$ is also a subgroup of order 7
why? it could be a coset.

so $a K a^{-1} = K$ for all $a \in G$

so $K \trianglelefteq G$

Sylow also tells us that there is a subgroup Q with $|Q| = 3$

$Q \cong C_3$

As 7 and 3 are coprime, then $K \cap Q = \{e\}$

So now apply Recogn. criterion to conclude that

$G \cong K \rtimes_h Q$

$\cong C_7 \rtimes_h C_3$ for some h

Two lectures ago showed, that therefore

$G \cong C_7 \times C_3$

or $G \cong G(21) = \langle 2y \mid a^7 = 1, y^3 = 1, y a y^{-1} = a^2 \rangle$

QED

n	G with $ G = n$	Complete?
1	$\{1\}$	✓
2	C_2	✓
3	C_3	✓
4	$C_4, C_2 \times C_2$	✓
5	C_5	✓
6	C_6, D_3	✓
7	C_7	✓

n	G with G = n	complete
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$?
9	$C_9, C_3 \times C_3$?
10	C_{10}, D_{10}	✓
11	C_{11}	✓
12	$C_{12}, C_2 \times C_6, D_{12}, A_4, D_6^*$?
13	C_{13}	✓
14	C_{14}, D_{14}	✓
15	$C_{15} = C_5 \times C_3$	
16	REAL MESS	
17	C_{17}	✓
18	A BIT OF A MESS	
19	C_{19}	✓
20		
21	$C_{21}, G(21)$	✓
22	C_{22}, C_{22}	✓
23	C_{23}	✓
24	DO ABLE	
25	$C_{25}, C_5 \times C_5$	
26	C_{26}, D_{26}	✓
27	REAL MESS	
28	EVEN APPEARED IN EXAM	
29	C_{29}	✓

Def Binary Dihedral groups:

D_{2n}^* has order $4n$
 $D_{2n}^* = \langle xy \mid x^n = 1, y^{n+1} = 1, yx = x^{n-1}y \rangle$

(Compare with $D_{2n} = \langle xy \mid x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$)

Prop. let G be a group with $|G| = 15$

then $G \cong C_{15} \cong C_5 \times C_3$

Proof (by Sylow counting)

If $15 = 5 \times 3$ go for the largest prime first

By Sylow, \exists subg. K $|K| = 5$ ($K \cong C_5$)
and $\exists \phi$ $|Q| = 3$

Sylow (ii) says that either $N_5 = 1$ or $N_5 \geq 6$

If $N_5 \geq 6$ then G has at least $6 \times (5-1) = 24$ elements of order 5

contradiction. So $N_5 = 1$

So K is unique subgroup of order 5
~~is~~ N

If $x \in G$ xKx^{-1} also a subgroup of order 5
so $xKx^{-1} = K$ $K \triangleleft G$

$K \cap Q = \{e\}$ $|Q| + |K| = |KQ|$

so $G \cong K \rtimes Q \cong C_5 \times C_3$

How many possibilities for h
 $h: C_3 \rightarrow \text{Aut}(C_5) \cong C_4$

h must be

so $G \cong C_5 \times C_3 \cong C_{15}$

Q.E.D.

Group actions and the class equation

22/01/11

Defn Let G be a group
 X be a set

By a (left) **action of G on X** we mean a mapping
 $\circ: G \times X \rightarrow X$

[$g \cdot x$ rather than $\circ(g, x)$]

- s.t.
- 1) $(gh) \cdot x = g \cdot (h \cdot x)$ $g, h \in G, x \in X$
 - 2) $1 \cdot x = x$ $x \in X$

examples: 1) **left translation**

$X = G$, $\circ =$ group multiplication

$$G \times G \rightarrow G$$

$$g \cdot x = gx$$

2) **Right translation**

Again $X = G$

$$G \times G \rightarrow G$$

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

$$(gh) \cdot x = x(gh)^{-1}$$

$$= (xh^{-1})g^{-1}$$

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

$$(gh) \cdot x = g \cdot (h \cdot x)$$

3) **Conjugation** (interesting example)

Again $X = G$, but

$$\ast: G \times G \rightarrow G$$

combines both left and right translation

$$g \ast x = g a g^{-1}$$

Def-n. Orbit of an element

let $\cdot : G \times X \rightarrow X$ be an action
 $x \in X$

Define $\langle x \rangle = \{g \cdot x : g \in G\}$ - is the orbit of x
 under the action

Example

let $G = X = D_6$ and consider the action by conjugation

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

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

let's compute the orbits!

$$G = D_6 = X = \{1, a, a^2, y, ay, a^2y\}$$

$$x^3 = y^2 = 1, \quad yx = a^2y$$

Take each element of $X (= D_6)$ and look at its orbit:

$$1) \langle 1 \rangle = \{g \cdot 1 : g \in D_6\} = \{1\}$$

$$2) \langle a \rangle = \{g \cdot a : g \in D_6\} = \{1 \cdot a^{-1}, a \cdot a^{-1}, a^2 \cdot a^{-1}, y \cdot a y^{-1}, (ay) \cdot a (ay)^{-1}, (a^2y) \cdot a (a^2y)^{-1}\} =$$

$$= \{a, a, a, a^2, a^2, a^2\}$$

$$\langle a \rangle = \{a, a^2\}$$

$$3) \langle a^2 \rangle = \{1 \cdot a^2 \cdot 1^{-1}, a \cdot a^2 \cdot a^{-1}, a^2 \cdot a^2 \cdot a^{-2}, y \cdot a^2 \cdot y^{-1}, (ay) \cdot a^2 \cdot (ay)^{-1}, (a^2y) \cdot a^2 \cdot (a^2y)^{-1}\}$$

$$= \{a^2, a^2, a^2, a, a, a\}$$

$$\langle a^2 \rangle = \{a, a^2\}$$

$$4) \langle y \rangle = \{ (y y^{-1}), (a y a^{-1}), (a^2 y a^{-2}), (y y y^{-1}), (a y a^{-1} (a y)^{-1}), ((a^2 y) y (a^2 y)^{-1}) \} = \\ = \{ y, a^2 y, a y, y, a^2 y, a y \} \\ \text{i.e. } \langle y \rangle = \{ y, a y, a^2 y \}$$

$$5) \langle a y \rangle = \{ y, a y, a^2 y \}$$

$$6) \langle a^2 y \rangle = \{ y, a y, a^2 y \}$$

To summarise:

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

$$\langle a \rangle = \{ a, a^2 \} = \langle a^2 \rangle$$

$$\langle y \rangle = \{ y, a y, a^2 y \} \quad (\langle a y \rangle = \langle a^2 y \rangle)$$

So these orbits $\langle 1 \rangle, \langle a \rangle, \langle y \rangle$

Notice (again) **distinct orbits have empty intersection.**

$$\text{e.g. } \langle 1 \rangle \cap \langle a \rangle = \emptyset$$

$$\langle 1 \rangle \cap \langle y \rangle = \emptyset$$

$$\langle a \rangle \cap \langle y \rangle = \emptyset$$

~~The~~ **class**

The class equation for this action:

$$X = |\langle 1 \rangle| + |\langle a \rangle| + |\langle y \rangle| \quad \text{— set theoretic version}$$

Numerical version of class equation

$$|X| = |\langle 1 \rangle| + |\langle a \rangle| + |\langle y \rangle|$$

$$6 = 1 + 2 + 3$$

In general
Given $\circ : G \times X \rightarrow X$ action

Prop. let $x, y \in X$
then either (i) $\langle x \rangle = \langle y \rangle$
(ii) $\langle x \rangle \cap \langle y \rangle = \emptyset$

(In English, distinct orbits are disjoint)

Proof:

ETP that if $\langle x \rangle \cap \langle y \rangle \neq \emptyset$, then $\langle x \rangle = \langle y \rangle$

enough to
prove

Suppose $z \in \langle x \rangle \cap \langle y \rangle$
 $z \in \langle x \rangle$ so $z = g \circ x$ for some $g \in G$

Also $z \in \langle y \rangle$ so $z = h \circ y$ for some $h \in G$

So $g \circ x = h \circ y$ for some $g, h \in G$

$$g^{-1} \circ (g \circ x) = (g^{-1} h) \circ y \quad g^{-1} \circ (h \circ y) = g^{-1} \circ (h \circ y)$$

$$x = (g^{-1} h) \circ y \quad (g^{-1} \circ h) \circ x = (g^{-1} h) \circ y$$

$$x \circ x = g^{-1} h \circ y \Rightarrow x =$$

let $r \in G$ $r \circ x = (r g^{-1} h) \circ y$
so $\langle x \rangle \subset \langle y \rangle$

Conversely $y = (h^{-1} g) \circ x$
for all $r \in G$ $r \circ y = (r h^{-1} g) \circ x$
so $\langle y \rangle \subset \langle x \rangle$
so $\langle x \rangle \subset \langle y \rangle \subset \langle x \rangle$
so $\langle x \rangle = \langle y \rangle$ QED

notice if $x \in X$ $a \in \langle x \rangle$

So $X = \bigcup_{x \in X} \langle x \rangle$ orbit representation

defn let $x_1, \dots, x_m \in X$ s.t. such that $\langle x_i \rangle \cap \langle x_j \rangle = \emptyset$ if $i \neq j$
 and such that for each $x \in X$
 $\exists i$ $x \in \langle x_i \rangle$
 i.e. $\langle x_1 \rangle, \langle x_2 \rangle, \langle x_3 \rangle, \dots, \langle x_m \rangle$ lists all distinct orbits

\Rightarrow set theoretic form eqn (0 version)
 $X = \bigsqcup_{i=1}^m \langle x_i \rangle$ Disjoint union
 Numerical form (1st version)
 $|X| = \sum_{i=1}^m |\langle x_i \rangle|$

example: let $X = G = D_6$, acting on itself by conjugation
 the orbits are

$$\{1\}, \{x, x^2\}, \{y, xy, x^2y\}$$

One choice of orbit reps

$$x_1 = 1, x_2 = x, x_3 = y$$

So we thus have

$$X = \langle 1 \rangle \cup \langle x \rangle \cup \langle y \rangle$$

choice not unique in general. could also take

$$x_1 = 1, x_2 = x^2, x_3 = xy$$

$$X = \langle 1 \rangle \cup \langle x^2 \rangle \cup \langle xy \rangle$$

Numerical class eqn here is

$$6 = 1 + 2 + 3$$

(no double counting. Different orbits are Disjoint)

Defn - more useful form of class eqn

$\therefore G \times X \rightarrow X$ action

let $x \in X$.

Define $G_x = \{g \in G, g \cdot x = x\}$ - stability group of x
Isotropy group of x

Prop G_x is a subgroup of G

Proof:

1) $x = x$ so $1 \in G_x$

2) $g, h \in G_x$ then

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

$h \in G_x \quad g \in G_x$

so $gh \in G_x$

3) let $g \in G_x$

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

so $g^{-1} \cdot x = x$ so $g^{-1} \in G_x$ Q.E.D.

Example let $X = G = D_6$ acting on itself by conjugation

$$X = \{1, x, x^2, y, xy, x^2y\} = D_6$$

$$G_x = \{g \in D_6; g \cdot x \cdot g^{-1} = x\}$$

$$\begin{array}{lll}
 x x^{-1} = e & x \in G_2 & y z y^{-1} = z^2 \\
 x x^{-1} = e & x \in G_2 & y \notin G_2 \\
 x^2 x^{-2} = e & x^2 \in G_2 & x y \notin G_2, x^2 y \notin G_2
 \end{array}$$

So $G_2 = \{1, x, x^2\}$

G_y ?? $1 \in G_y$

$$\begin{array}{ll}
 y y y^{-1} = y & y \in G_y \\
 x y x^{-1} = x y \neq y & x \notin G_y
 \end{array}$$

define $G_y = \{1, y\}$

W/ check

$$\begin{array}{l}
 G_1 = D_6 \\
 G_2 = \{1, x, x^2\} = G_{x^2} \\
 G_y = \{1, y\} \\
 G_{xy} = \{1, xy\} \\
 G_{x^2y} = \{1, x^2y\}
 \end{array}$$

Prop $\text{let } \cdot : G \times X \rightarrow X$ be an action
let $z \in X$, then there is a **bijection**
 $G/G_z \leftrightarrow \langle z \rangle$

Proof

The elements of G/G_z are subsets of G of the form
 $g \cdot G_z = \{g a : a \in G_z\}$

Recall that $g \cdot G_z = h \cdot G_z$ \iff $h^{-1}g \in G_z$ \iff Rule of equality

Define a mapping $\eta : G/G_z \rightarrow \langle z \rangle$
 by $\eta(g \cdot G_z) = g \cdot z$

ψ is well defined:

Suppose $g \cdot g_2 = h \cdot g_2$, then
 $h^{-1}g \in G_2$ so $(h^{-1}g) \cdot z = z$
 $(h^{-1}g) \cdot z = z$
 $g \cdot z = h \cdot z$

so I get same answer if I represent a coset in a different way.

ψ obviously surjective by Def'n of $\langle z \rangle$ no many comparisons no many?

Go to show ψ is injective

no before
no
no

Suppose $\psi(g \cdot G_2) = \psi(h \cdot G_2)$
 so $g \cdot z = h \cdot z$
 so $(h^{-1}g) \cdot z = z$

so $h^{-1}g \in G_2$ so $g \cdot G_2 = h \cdot G_2$
 i.e. ψ is injective
 hence bijective Q.E.D

why $|g/S_2| = |g/S_1|$

Corollary $|\langle z \rangle| = |G|/|G_2|$

check with the action of D_6 on itself by conjugation

Three orbits $\langle 1 \rangle, \langle x \rangle, \langle y \rangle$
 $|\langle 1 \rangle| = 1$ $|\langle x \rangle| = (D_6)/G_2 = 6/2 = 3$

$\langle x \rangle = \{x, x^2\}$ $|\langle x \rangle| = 2 = 6/3$
 $G_2 = \{1, x, x^2\}$ $|G_2| = 3$

$$\langle y \rangle = \{y, ay, a^2y, \dots\}$$

$$G_y = \{1, y\} \quad |G_y| = 2$$

$$|\langle y \rangle| = 3 = 6/2$$

Really useful theorem of orbit-stabilizer

Proof Let $\cdot : G \times X \rightarrow X$ action | G finite
| X finite

Let x_1, \dots, x_m be a set of orbit representatives.

Then $|X| = \sum_{i=1}^m \frac{|G|}{|G_{x_i}|}$

Proof $|X| = \sum_{i=1}^m |O_{x_i}|$

$|O_{x_i}| = |G|/|G_{x_i}|$ so substitute back
Q.E.D.

Defn Fixed Point set of an action

Let $\cdot : G \times X \rightarrow X$ be an action
Define $X^G = \{x \in X : \forall g \in G, g \cdot x = x\}$

X^G is the fixed point set

Another way of saying this is that
 $x \in X^G \Leftrightarrow \langle x \rangle = \{x\}$

Prop.

1st Real application of Eqn $Eq-n$:

let p be a prime
 G be a group $|G| = p^n$
 acting on a finite set X
 then $|X| \equiv \sum |X^g| \pmod{p}$

Proof: $\because G \times X \rightarrow X$ is the action
 choose a set of orbit representatives
 x_1, \dots, x_m

choose them in such a way that fixed points come first
 i.e. $X^g = \{x_1, \dots, x_k\}$ $k \leq m$ if there is no

and $x_i \notin X^g$ $k < i$ ~~set~~ fixed point
 in a set.
 $\langle x_r \rangle = \{x_r\}$ for $1 \leq r \leq k$
 $|\langle x_r \rangle| = 1$ for $1 \leq r \leq k$

whilst $G_{x_i} \neq G$ for $k < i$
 $x \in X^g \iff G_x = G$

Write down the class Eqn
 $|X| = \sum_{r=1}^k |\langle x_r \rangle| + \sum_{i>k} |G|/|G_{x_i}|$

$$|X| = k + \sum_{i>k} |G|/|G_{x_i}|$$

$$|G| = p^n \implies |G_{x_i}| = p^{n_i} \quad n_i \leq n$$

and since $|G_{x_i}| \neq |G|$ $k < i$

$$\text{Then } p^{n_i} < p^n \quad k < i$$

$$p^{n-m} \equiv 0 \pmod{p} \quad k < l$$

$$|X| = k + \sum_{i>k} p^{n-m_i}$$

$$|X| \equiv k \pmod{p} \quad (|X| \equiv |X^g| \pmod{p})$$

$$|X| = |X^g|$$

Q.E.D

01/03/11

Application of class Eq-n
Then Wilson's Theorem.

let p be a prime
 $0 < k < p$ be an integer ($k \in \mathbb{N}$)

$$\binom{kp^n}{p^n} \equiv k \pmod{p}$$

Proof:

let G be a group of order p^n (e.g. the cyclic group)
 $X = G \times \{1, \dots, k\}$; $|X| = p^n \cdot k$

consider the action

$$\begin{aligned} \therefore G \times X &\rightarrow X \\ (g \cdot h, i) &= (gh, i) \quad \begin{matrix} h \in G \\ i \in \{1, \dots, k\} \end{matrix} \end{aligned}$$

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

Q: How big is \mathcal{X} ?

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

G also acts on X as follows:

let $G \times X \rightarrow X, (g, A) \rightarrow g \cdot A$
 be the action $g \cdot A = \{g a : a \in A\}$, where $A \in X$

To prove Wilson's theorem enough
 to show $|X^G| = k$

$$|X| = |X^G| \pmod{p}$$

$$1 \rightarrow 1$$

$$s \rightarrow t$$

$$t \rightarrow st$$

$$st \rightarrow s$$

Since $|G| = p^n$
 By last lecture
 $|X| \equiv |X^G| \pmod{p}$
 since $|X| = \binom{kp^n}{p^n}$

$$k \binom{kp^n}{p^n} \equiv k \pmod{p}$$

let $A \in X^G$ i.e. $g \cdot A = A$
 choose some element $a \in A$ $h \in G$
 a has form $a = (h, i)$ $1 \leq i \leq k$

For each $g \in G$, $g \cdot (h, i) \in A$
 i.e. $(gh, i) \in A$
 every element $\lambda \in G$ can be written in form $\lambda = gh$
 ($h = g^{-1}\lambda$)

So for every $\lambda \in G$, $(\lambda, i) \in A$

So $G \times \{i\} \subset A$

But $|G| = p^n = |A| \Rightarrow H = G \times \{i\}$
 i.e. every fixed point of X has form $G \times \{i\}$

So $X^G = G \times \{1\}, G \times \{2\}, \dots, G \times \{k\} \Rightarrow |X^G| = k$
Q.E.D.

Theorem Sylow Part I

Let p be a prime
 $k \geq 1$ be coprime to p
 G be a group $|G| = kp^n$
 then \exists subgroup H of $G : |H| = p^n$

Proof:

Let \mathcal{P} be the set of subsets of G of order p^n

$$\mathcal{P} = \{A \subseteq G : |A| = p^n\}$$

$$\text{so } |\mathcal{P}| = \binom{kp^n}{p^n}$$

{proof goes by induction on k }
 For $k=1$ there is nothing to prove

so suppose $k > 1$ and the statement is already proved for groups of order $k'p^n$ $1 \leq k' < k$

let G act on \mathcal{P} by
 $G \times \mathcal{P} \rightarrow \mathcal{P}$
 $g \cdot A = \{gag : a \in A\}$
 ← mult. in G

$$\text{Since } k > 1 \quad \binom{kp^n}{p^n} > kp^n$$

so there is more than one orbit in \mathcal{P}

let A_1, \dots, A_m be a set of orbit rep in \mathcal{P} for the above action

let $G_2 = g_{A_i} = \{g \in G : gA_i = A_i\}$

The class eq - n now gives

$$|P| = |g|/|g_1| + \dots + |g|/|g_m| = \sum_{i=1}^m |g|/|g_i| \quad (m > 1)$$

$$|g| = kp^n \quad |g_i| = k_i p^{e_i} \quad e_i \leq n$$

and $k_i < k$
(k_i div k)

$$\text{So } \binom{kp^n}{p^{e_i}} = \sum_{i=1}^m \binom{k}{k_i} p^{n-e_i}$$

By Wilson's Thm

$$k \equiv \sum_{i=1}^m p^{n-e_i} \pmod{p}$$

If each $e_i < n$ then
 RHS $\equiv 0 \pmod{p}$
 LHS $\equiv k \not\equiv 0 \pmod{p}$

Contradiction

so for some i $e_i = n$
 $|g_i| = k_i p^n \quad k_i < k$

Now appeal to Induction hypothesis

g_i is a group of order $k_i p^n \quad k_i < k$

so g_i has a subgroup H

$$|H| = p^n$$

$$H \subset g_i \subset g$$

So H is a subgroup of G
 $|H| = p^n$

Q.E.D

Theorem Sylow Part II

let p be a prime
 $k \geq 1$ is a coprime to p
 G be a group $|G| = kp^n$
 Put $N_p =$ no of subgroups of order p^n
 then $N_p \equiv 1 \pmod{p}$

Proof

let S denote the set
 $S = \{Q \leq G : |Q| = p^n \text{ and } Q \text{ is a subgroup}\}$
 $|S| = N_p$ (def-n of N_p)
 $S \neq \emptyset$ by Sylow Part I

let $P \in S$ (by Sylow I, $S \neq \emptyset$)

i.e. P is a subgroup of G $|P| = p^n$

Consider the following action of P on S
 $P \times S \rightarrow S$

$$g \cdot Q = gQg^{-1} \quad (g \in P, Q \in S)$$

Since $|P| = p^n$ then
 $|S^P| \equiv |S| \pmod{p}$

$$S^P = \{Q \in S : gQg^{-1} = Q \text{ for all } g \in P\}$$

$$N_P \equiv |S^P| \quad (\text{fixed } P) \quad \text{by def-}n$$

To complete the proof we must show there is only one fixed point under the action

$$\therefore \text{O. } |S^P| = 1$$

Then $N_P = \text{mod } P$

4/03/11

clearly $P \in S^P$
 If $g \in P$ $gPg^{-1} = P$

got to show that if $Q \in S^P$ then $Q = P$

so let $Q \in S^P$ ($\forall g \in P$ $gQg^{-1} = Q$)

consider product $PQ = \{pq : p \in P, q \in Q\}$

I claim: PQ is a subgroup of G
 $1 = 1 \cdot 1 \in PQ$

~~subgroup~~ Suppose $p_1, q_1 \in PQ$ $p_2, q_2 \in PQ$

$$(p_1, q_1)(p_2, q_2) = p_1 p_2 (p_2^{-1} q_1 p_2) q_2$$

$$p_2^{-1} \in P \quad q_1 \in Q \quad \text{so } p_2^{-1} q_1 p_2 \in Q$$

$$p_1 p_2 \in P \quad p_2^{-1} q_1 p_2 q_2 \in Q$$

so $(p_1, q_1)(p_2, q_2) \in PQ$

let $pq \in PQ$ $(pq)^{-1} = q^{-1}p^{-1}$
 $= p^{-1}(pq^{-1}p^{-1})$

$p^{-1} \in P$ $pq^{-1}p^{-1} \in Q$ $\therefore (pq)^{-1} \in PQ$

QED (PQ is a subgroup)

Observe that $P \subset PQ$ and $Q \subset PQ$

consider PQ/Q . How big it is?

consider also $P/P \cap Q$ ($P \cap Q$ is a subgroup of P)

I claim that $|P/P \cap Q| = |PQ/Q|$

Define $\nu: P/P \cap Q \rightarrow PQ/Q$ $x \in P$

(concentrate on Rule of equality for cosets)

$\nu(x(P \cap Q)) = xQ$

- Need to show
- i) ν is well defined
 - ii) ν is injective
 - iii) ν is surjective

well defined suppose that $x(P \cap Q) = (x')(P \cap Q)$

then $x^{-1}x' \in P \cap Q \subset Q$

So $\alpha^{-1} \alpha' \in Q$

So $\alpha Q = \alpha' Q$ Q.E.D. well defined

ii) Injective:

suppose $\alpha(p(P \cap Q)) = \alpha(y(P \cap Q))$

$\alpha Q = y Q$

so $y^{-1} \alpha \in Q$ But $\alpha, y \in P \Rightarrow y^{-1} \alpha \in P$

so $y^{-1} \alpha \in P \cap Q$ so $\alpha(P \cap Q) = y(P \cap Q)$
Q.E.D. injectivity

iii) Surjective:

let $p q \in P Q / Q$
 $q Q = Q$

so $p q Q = p Q = \alpha(p(P \cap Q))$
Q.E.D. surjectivity

conclusion: already shown $|P/P \cap Q| = |PQ/Q|$

$|P| = p^h$ so $|P/P \cap Q| = p^{h-e}$ where $|P \cap Q| = p^e$

so $|PQ/Q| = p^{h-e}$

so $|PQ| = |Q| p^{h-e} = p^{2h-e}$

But PQ is a subgroup of G

$$|PQ| = p^{2n-e} \quad |G| = kp^n \quad p \nmid k$$

$$\text{So } 2n - e \leq n$$

But $P \subset PQ$ so $p^n \leq p^{2n-e}$

$$\therefore n \leq 2n - e \leq n$$

$$\therefore e = n$$

$$\text{and } |PQ| = p^n (= p^{2n-n})$$

$$P \subset PQ \quad (P) = (PQ)$$

$$\text{So } PQ = P$$

$$Q \subset PQ \quad (Q) = (PQ)$$

$$\text{So } PQ = Q$$

$$\text{So } P = Q \quad \& \quad \$P = \{P\}$$

i.e. P is unique fixed point

$$|SP| = 1$$

$$\therefore \#P = 1 \pmod{p}$$

QED Fin.



A large grid of blue horizontal lines on a white background, with a vertical red margin line on the left side. The grid is intended for writing mathematical solutions or notes.

Q1/18
Defn

Ring Theory

$X \times X \rightarrow X$
 $(x, y) \rightarrow x \cdot y$
 $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
 X is a set

$\left. \begin{array}{l} \text{semi-group} \\ \text{monoid} \end{array} \right\}$

$\left. \begin{array}{l} \text{2) assume } \{ \text{s.t. } 1 \cdot x = x \cdot 1 = x \\ \exists 1 \in X \end{array} \right\}$

So $(X, \cdot, 1)$ is called **monoid** (multiplicative)

if $\forall x \exists y : xy = 1 = yx$ **Inverses** \Rightarrow **Group** (it is a group)

ex: Take \mathbb{Z} : Two operations

- $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ 0 identity - a inverse
Additive group
- $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ 1 identity don't have inverse
multiplicative monoid.

both commutative
 $x \cdot (y + z) = xy + xz$

Def-n By a **ring** \mathcal{R} we mean $\mathcal{R} = (\mathcal{R}, +, 0, \cdot, 1)$ where

- 1) \mathcal{R} is a set $\{x, y\} \in \mathcal{R}$
- 2) $+ : \mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$ commutative group operation with 0 - additive identity
- 3) $(\mathcal{R}, \cdot, 1)$ is a multiplicative monoid
- 4) $x \cdot (y + z) = x \cdot y + x \cdot z$
 $(y + z) \cdot x = y \cdot x + z \cdot x$
Distributive law

Note: We will consider only commutative rings
 (i.e. $\forall x, y \in \mathcal{R} \quad x \cdot y = y \cdot x$)

standard example: 1) \mathbb{Z}

2) fields eg $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are also rings, but they are (not typical) too specific

[We'll use Ring theory to construct new fields]

A non commutative example:

Let R be a ring (any ring!)

$$M_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a noncommutative ring (provided $n \geq 2$)

Defn Polynomial rings:

Let F be a field (e.g. $F = \mathbb{Q}, \mathbb{F}_2, \mathbb{F}_p$)

$$F[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in F\}$$

add & multiply in obvious way

More generally if R is a ring

$$R[x] = \left\{ \sum_{r=0}^n a_r x^r \mid a_r \in R \right\}, n \geq 0$$

ring of polynomials with coef-nts in R

e.g. $\mathbb{F}_2[x], \mathbb{Z}[x]$

Defn of field \mathbb{F} is a ring in which
 $x \neq 0 \Rightarrow \exists x^{-1} \in \mathbb{F} : x x^{-1} = 1 \quad x^{-1} x = 1$

e.g. 1) \mathbb{Q} field
 2) \mathbb{F}_p field with p elements p prime
 $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ (+ addition & multiplication p)
 Coming soon!!! \mathbb{F}_{p^2} field with p^2 elements

Quotient Rings 08/03/11
 start with two examples:
 i) \mathbb{Z} ii) $\mathbb{F}[x]$ ring of polynomials in x
 with coeff-nts in a field \mathbb{F} .

Notation $\mathbb{Z}/n \equiv \text{Arithmetic mod } n$

Divide any integer by n to get a remainder r
 $0 \leq r < n$
 Add & multiply remainders except we put $n \equiv 0$

example 1) $\mathbb{Z}/3 = \{0, 1, 2\}$

normally \downarrow comp. \mathbb{Z}_3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

is a field
 alternatively
 written \mathbb{F}_3

10/10/20 in 30 mins

2) $\mathbb{Z}/4 = \{0, 1, 2, 3\}$, $\mathbb{Z}/4$ (for mult.) is not a field
It is not written \mathbb{F}_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

+	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

3) However there is a field \mathbb{F}_4
Start with \mathbb{F}_2 with elements
 $\mathbb{F}_2 = \{0, 1\}$

Take $\mathbb{F}_2[x] / x^2 + x + 1$

We have possible remainders after dividing by $x^2 + x + 1$
Add & multiply out etc.

$x^2 + x + 1 \equiv 0$

equivalently write

$x^2 \equiv -(x+1)$

equivalently

$x^2 = x+1$

($1 = -1$ in \mathbb{F}_2)

have one polynomial
note! 2
cont. $(10 \frac{1}{2} 4)$

Possible remainders are polyn-als of deg ≤ 1
over \mathbb{F}_2 , these are $0, 1, x, x+1$

worksheets:

+	0	1	x	$x+1$
0	0		x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

·	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

0 in \mathbb{F}_2
 $(x+1)(x+1) = x^2 + 2x + 1 = (x+1) + 1 = x$
 $x^2 \equiv x+1$ (from above)

$\mathbb{F}_2[x]/x^2+x+1$ is a field. This is \mathbb{F}_4

4) Contrast this with $\mathbb{F}_2[x]/x^2+1$ elements look the same $\{0, 1, x, x+1\}$

worksheets:

·	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	x
$x+1$	0	$x+1$	x	0

$x^{2+1} \equiv 0$
 $x^2 \equiv -1$
 $x^2 \equiv 1$ over \mathbb{F}_2

not a field $x+1$ has no inverse

Def-m If R is a ring, the unit group R^* is the set of invertible elements under multiplication

$R^* = \{a \in R : \exists b \in R \text{ s.t. } ab = ba = 1\}$

R is a field $\Leftrightarrow R^* = R - \{0\}$

Example $\mathbb{F}_3[x]/x^2+1$ $\mathbb{F}_3 = \{0, 1, 2\}$

Possible remainders:

- 0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2

$x^2+1 \equiv 0 \Leftrightarrow x^2 = -1 \Leftrightarrow x^2 \equiv 2$

finish:

row 3)
column 4)
no 0,0

	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	x+1
x+1	0	x+1	2						
x+2	0	x+2							
2x	0	2x							
2x+1	0	2x+1							
2x+2	0	2x+2							

Some Prof

$\mathbb{Z}/n \Leftrightarrow \mathbb{F}_n[x]/p(x)$ $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$
 (is a field, when n is prime)

working!

is a field iff
 irreducible / \mathbb{F}

Defn $p(x) = a_n x^n + \dots + a_1 x + a_0$ is irreducible / \mathbb{F} , when
 there is no factorisation $p(x) = a(x) b(x)$

- e.g. 1) x^2+x+1 is irred. / \mathbb{F}_2
- 2) $x^2+1 = (x+1)^2$ is not irred. / \mathbb{F}_2

where $\deg(a) < n$ and $\deg(b) < n$
 3) hence x^2+1 is irred. / \mathbb{F}_3

4) $\mathbb{R}[x]/x^2+1 \cong \mathbb{C} \rightarrow x^2+1$ is irred. / $\mathbb{R}[x]$
 $\Rightarrow \mathbb{R}[x]/x^2+1$ is a field
 why it is

11/03/11

A ring $R = (R, +, \cdot, 0, 1)$

consists of following data

i) $(R, +, 0)$ is an abelian group
 $+$: $R \times R \rightarrow R$ assoc, commut, $0 \in R$ Identity
 $\forall x \in R \exists -x \in R \quad x + (-x) = 0$

ii) $(R, \cdot, 1)$ monoid
 \cdot is assoc. (needn't be commut. in general)
 1 identity

iii) $x \cdot (y+z) = xy + xz$
 $(y+z) \cdot x = yx + zx$

Defn If R, S are rings, by a ring homomorphism $\varphi: R \rightarrow S$ we mean a mapping such that

- (i) $\varphi(x+y) = \varphi(x) + \varphi(y)$
 - (ii) $\varphi(xy) = \varphi(x)\varphi(y)$
 - (iii) $\varphi(1) = 1$
- } $\forall x, y \in R$

why?

Automatically true that $\varphi(0) = 0$ from (i) & (ii)

Defn $\varphi: R \rightarrow S$ is a ring isomorphism when φ is a bijective homomorphism.

Defn $(R, +, 0, \cdot, 1)$ is a subring of $(S, +, 0, \cdot, 1)$ when

- $(R, +, 0)$ is a subgroup of $(S, +, 0)$
- $(R, \cdot, 1)$ is a submonoid of $(S, \cdot, 1)$

e.g. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a collection of subrings

Suppose K is a subgroup of G
 $G/K = \{xK : x \in G\}$
 G/K is a group when $K \triangleleft G$

M notes: cosets; we need proof

$$G/K \times G/K \rightarrow G/K$$

$$(x \cdot K) \cdot (y \cdot K) = xy \cdot K$$

what does it mean w.r.m

Question: let R be a ring
 suppose $I \subset R$ is a subset
 what properties we need for I in order, that
 R/I is a ring (naturally)?

clearly need I to be an additively subgroup of R
 so R/I is an additively group
 what about mult. on R/I ?

necessary

Def-n let R be a ring (commutative) $I \subset R$

Say that I is an ideal in R when

- (i) I is an additive subgroup of R
 (i.e) 1) $0 \in I$ 2) if $x, y \in I$, $x+y \in I$
 3) if $x \in I$ then $-x \in I$
- (ii) if $x \in I$ and $\lambda \in R$,
 then $\lambda x \in I$
 (so $\lambda^2 \in I \oplus R$ commutative)

Prop let I be an ideal in R
 then R/I has a ring structure, with property
 that $\eta : R \rightarrow R/I$
 $\eta(x) = x+I$ is a ring homomorphism

which means
 ↑

Observe: we write cosets additively $x+I$, because
 I is additive subgroup of R

Proof:
 We need to define:

Prop

- i) $+$: $R/I \times R/I \rightarrow R/I$
- ii) a 'zero-element' in R/I
- iii) \cdot : $R/I \times R/I \rightarrow R/I$
- iv) a 'unit element' in R/I

(i) comes from the fact that I is normal or an additive subgroup

$$x + I = I + x$$

So we define: $(x+I) + (y+I) = (x+y) + I$

(ii) Zero the zero element is $0+I (=I)$

(iii) Define $(x+I) \cdot (y+I) = xy + I$

Need to check that \cdot is well defined i.e. answer is independent of way you've represent cosets.

$$x + I = x' + I \Leftrightarrow x - x' \in I$$

Suppose $x_1 + I = x_2 + I$
and $y_1 + I = y_2 + I$

got to show $x_1 y_1 + I = x_2 y_2 + I$
(i.e. got to show $x_1 y_1 - x_2 y_2 \in I$)

$$\begin{aligned} \text{Then: } x_1 y_1 - x_2 y_2 &= \\ &= (x_1 - x_2) y_1 + x_2 (y_1 - y_2) \end{aligned} \quad \Downarrow \text{R comput.}$$

$x_1 - x_2 \in I$ so $y_1(x_1 - x_2) \in I$ (I ideal)
 $y_1 - y_2 \in I$ so $x_2(y_1 - y_2) \in I$

I is additive subgroup so

$$x_1 y_1 - x_2 y_2 = \underbrace{y_1(x_1 - x_2)}_I + \underbrace{x_2(y_1 - y_2)}_I \in I$$

So $x, y, + \mathcal{I} = x, y, + \mathcal{I}$
and multiplication is well defined

(iv) Take $\varphi = \text{Quotient ring}$
 $\varphi(x+y) = (x+y) + \mathcal{I} = (x+\mathcal{I}) + (y+\mathcal{I})$

φ is tautologically a ring homomorphism

$$\varphi(x+y) = (x+y) + \mathcal{I} = (x+\mathcal{I}) + (y+\mathcal{I}) = \varphi(x) + \varphi(y)$$

$$\varphi(xy) = (xy) + \mathcal{I} = (x+\mathcal{I})(y+\mathcal{I}) = \varphi(x)\varphi(y)$$

$$\varphi(1) = 1 + \mathcal{I} = 1$$

If \mathcal{I} is an ideal in R then R/\mathcal{I} is called the quotient ring of $R \text{ mod } \mathcal{I}$

Examples \mathbb{Z}/n

Take $R = \mathbb{Z}$
 $\mathcal{I} = \{ \lambda n : \lambda \in \mathbb{Z} \} (= (n))$

(n) is obviously ideal in \mathbb{Z}

Forming \mathbb{Z}/n , setting the ideal $(n) \equiv 0$
i.e. \cup ideal (n) everytime you see n write 0
Heuristic interpretation

WTF!
?

11/10/18
11/10/18
11/10/18
11/10/18

Example: $\mathbb{F}[x]/p(x)$ (e.g. $p(x) = x^2 + x + 1$)

where $\mathbb{R} = \mathbb{F}[x]$

$$\mathbb{I} = \{ \lambda(x)p(x); \lambda(x) \in \mathbb{F}[x] \}$$

i.e. multiples of $p(x)$

Example: $\mathbb{F}_3 = \{0, 1, 2\}$ field with 3 elements

$$\mathbb{F}_3[x]/x^2+1 \cong \mathbb{F}_3[x]/x^2+2x+2 = \mathbb{F}_3[y]/y^2+2y+2$$

$$\varphi(x) = y+1$$

isomorphism?

$$\begin{aligned} \varphi(x^2+1) &= \varphi(x)^2 + \varphi(1) = (y+1)^2 + 1 \\ &= y^2 + 2y + 1 + 1 \\ &= y^2 + 2y + 2 \end{aligned}$$

$$\begin{aligned} \varphi(x^2) &= \varphi(x \cdot x) = \\ &= \varphi(x) + \varphi(x) \end{aligned}$$

$\{1, x\}$ basis for $\mathbb{F}_3[x]/x^2+1$

$\{1, y\}$... $\mathbb{F}_3[y]/y^2+2y+2$

$$\varphi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$1 \rightarrow 1 \quad 2 \rightarrow 1+y$$

Need to check formally that

$$\varphi(a+bx)(c+dx) = \varphi(a+bx)\varphi(c+dx)$$

$$\varphi(a+bx) = (a+bx) + by$$

21/10-9 15/03/11

\mathbb{F} field $p(x) = a_n x^n + \dots + a_1 x + a_0$ $a_n \neq 0$
polynomial of deg. n / \mathbb{F} ($a_i \in \mathbb{F}$)

Question: when is $\mathbb{F}[x]/(p(x))$ a field?

Answer: Coming soon $\Leftrightarrow p(x)$ is irred. / \mathbb{F}

Prop. Any element of $\mathbb{F}[x]/(p(x))$ can be represented uniquely by a polynomial of deg $\leq n-1$

Proof: Write $I = (p(x)) = \{ \lambda(x) p(x) : \lambda(x) \in \mathbb{F}[x] \}$

Any element of $\mathbb{F}[x]/(p(x)) = \mathbb{F}[x]/I$

are represented in form $a(x) + I$ $a(x) \in \mathbb{F}[x]$
If $\deg a \geq n$ divide $a(x)$ by $p(x)$

using our division $a(x) = q(x) p(x) + a'(x)$ $\deg a'(x) \leq n-1$

So $a'(x) + I = a(x) + I$ and are represented $a(x) + I$ in desired form

This representation is unique because of $a'(x) + I = a''(x) + I$

and $\deg(a') \leq n-1$ $\deg(a'') \leq n-1$

$a'(x) - a''(x) \in I$ and $\deg(a' - a'') \leq n-1$

$a'(x) - a''(x) = \lambda(x) p(x)$ $\deg p = n$

so $\lambda(x) = 0$ and $a'(x) = a''(x)$ Q.E.D.

Corollary

$\mathbb{F}[x]/(p(x))$ (deg $p = n$) is a vector space over \mathbb{F}
and $\dim(\mathbb{F}[x]/(p(x))) = n$

Proof: Every element of $\mathbb{F}[x]/(p(x))$ is represented uniquely in form

is a vector space
Do a basis
Do a calculation

$$a_0 + a_1x + \dots + a_{n-1}x^{n-1} + I$$

So $\{1, x, \dots, x^{n-1}\}$ is a basis for $\mathbb{F}[x]/(p(x))$

Q.E.D.

Intermediate Stage

Def-n A commutative ring R is said to be an integral domain, when

for $a \in R, b \in R : ab = 0 \Rightarrow (a = 0) \text{ or } (b = 0)$

Note: every field is an integral domain, but not all integral domain is a field.

$(ab = 0 \text{ and } a \neq 0 \Rightarrow a^{-1}ab = 0 \Rightarrow b = 0)$

- e.g. 1) Any field is an integral domain
- 2) \mathbb{Z} is an int. \mathcal{D} .
- 3) If \mathbb{F} is a field $\Rightarrow \mathbb{F}[x]$ is an integral \mathcal{D} .
- 4) $\mathbb{Z}/4$ is not an integral \mathcal{D} .
 $2 \cdot 2 = 0$ but $2 \neq 0$.

Def-n

If $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ $a_n \neq 0$

say that $p(x)$ is irred. over \mathbb{F}

when there is no factorisation $p(x) = a(x)b(x)$ $a(x), b(x) \in \mathbb{F}[x]$

and $\deg(a) < n$ and $\deg(b) < n$

Intermediate prop.

let F be a field
 $p(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x] \quad a_n \neq 0$
 $\therefore F[x]/p(x)$ is an integral domain iff $p(x)$ is irred. / F

Proof:

\Rightarrow
 Suppose $p(x)$ is reducible i.e. $p(x) = a(x)b(x)$ $\deg a < n$
 $\deg b < n$

then

$I = (p(x))$
 $(a(x) + I)(b(x) + I) = a(x)b(x) + I = p(x) + I = I = 0$

but $a(x) + I \neq 0$
 $b(x) + I \neq 0$

QED.

\Leftarrow

Suppose $p(x)$ is irred. / F this part is more subtle
 Suppose $(a(x) + I)(b(x) + I) = 0$
 i.e. $a(x)b(x) \in I = 0$
 i.e. $a(x)b(x) \in I$
 i.e. $a(x)b(x) = \lambda(x)p(x)$ for some $\lambda(x)$ in $F[x]$

let $a(x) = a_1(x) \dots a_m(x)$
 $b(x) = b_1(x) \dots b_n(x)$
 factorization into irred.
 $\lambda(x)p(x) = a_1(x) \dots a_m(x) b_1(x) \dots b_n(x)$

By uniqueness of factorization
 $p(x) = a_i(x)$ or $p(x) = b_j(x)$ for some i, j

If $p(x) = a_i(x)$ $a(x) \in (p(x)) = \mathfrak{I}$
 $\Rightarrow a(x) + \mathfrak{I} = 0$

if $p(x) = b_j(x)$ $b(x) \in (p(x)) = \mathfrak{I}$
 $\Rightarrow b(x) + \mathfrak{I} = 0$

$(a(x) + \mathfrak{I})(b(x) + \mathfrak{I}) = 0$
 $\Rightarrow a(x) + \mathfrak{I} = 0$ or $b(x) + \mathfrak{I} = 0$ **Q.E.D**

Prop. Let R be a commutative integral dom.

Suppose R contains a field \mathbb{F} (as a subring)
 $[\dim_{\mathbb{F}}(R)$ is finite.]

then R is a field

Proof.

let $a \in R$ and $a \neq 0$

have to show $\exists b \in R$ s.t. $ab = 1$

let $T: R \rightarrow R$

$T(x) = ax$

T is linear over \mathbb{F}

so $\dim \ker T + \dim \text{Im } T = \dim R$

what is $\ker T$?

dimension
 field
 linear

$T(x) = 0 \Rightarrow ax = 0$
 But $a \neq 0$ and R integral domain

So $x = 0$

$\text{Ker } T = \{0\}$

So $\dim \text{Im } T = \dim R$

So $\text{Im } T = R$ (f.d)

T is surjective

So $\exists b \in R$ $T(b) = 1$

i.e. $\exists b \in R$ $ab = 1$

R is a field

Q.E.D.

Corollary $(\deg p = n)$
 $\mathbb{F}[x]/p(x)$ is a field $\Leftrightarrow \mathbb{F}[x]/p(x)$ integral domain
 $\Leftrightarrow p(x)$ i.r.d.

13/03/11

Theorem

Let \mathbb{F} be a field

Let $p(x) \in \mathbb{F}[x]$, $\deg(p) = n > 0$

Then following are equivalent:

(i) $\mathbb{F}[x]/p(x)$ is a field

(ii) $\mathbb{F}[x]/p(x)$ is an integral domain

(iii) $p(x)$ is irreducible over \mathbb{F}

Proof:

(i) \Rightarrow (ii) is obvious

(ii) \Rightarrow (i) in this case because $\mathbb{F}[x]/p(x)$ is a vector space of finite dimension n over \mathbb{F}

I showed last time that (ii) \Rightarrow (iii) QED

Beware hypothesis of finite dimensionality is essential here.

$F[x]$ has a Dom $\neq F$
 $F[x]$ is an integral domain but not a field.

Examples: 1) $F = \mathbb{C}$

let $p(x) \in \mathbb{C}[x]$, when $p(x)$ is irreducible?

Best proof: Answer: Fundamental theorem of Algebra. Gauss
 samuel's D'Alembert
 Alg vs theory
 iff $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$
 $p(x) = a_n (x - \lambda_1) \dots (x - \lambda_n)$ for some $\lambda_i \in \mathbb{C}$

2) $F = \mathbb{R}$

let $p(x) \in \mathbb{R}[x]$
 when is $p(x)$ irred / \mathbb{R}
 $p(x) = c(x - \lambda)$ $\lambda \in \mathbb{R}$
 $p(x) = a x^2 + b x + c$

Real Question: Given $a(x) \in \mathbb{R}[x]$

\Rightarrow when is $a(x)$ irred. over \mathbb{R} ?

No general answer except for an algorithm (being, but useful)

However there is a trick which gives quite often answers.

82 Eisenstein's criterion

let $a(x) = a_n x^n + \dots + a_1 x + a_0$
 be a polynomial over \mathbb{Z} ($a_i \in \mathbb{Z}$)
 Suppose there is a prime p st.
 (i) $a_n \not\equiv 0 \pmod{p}$
 (ii) $a_r \equiv 0 \pmod{p} \quad 0 \leq r \leq n-1$
 (iii) $a_0 \not\equiv 0 \pmod{p^2}$
 then $a(x)$ is irreducible / \mathbb{Q}

Example (Pythagoras)

let p be prime this is
 $x^2 - p$ is irred / \mathbb{Q}
 so $\mathbb{Q}[x] / \langle x^2 - p \rangle$ is a field.

$$\mathbb{Q}[x] / \langle x^2 - p \rangle \cong a + b\sqrt{p} \quad a, b \in \mathbb{Q}$$

$$x^2 = p \Leftrightarrow \sqrt{p} = x \quad (\sqrt{p})^2 = p$$

2) $p = 4$

$$x^5 + 14x^4 - 21x^2 + 35x + 4 \text{ is irred / } \mathbb{Q}$$

another trick:

$$x^4 + 11x^3 + 6x^2 + 4x + 3 = f(x) \text{ is irred / } \mathbb{Q}$$

$$(x+1)^4 + 2 = f(x)$$

write $g(y) = y^4 + 2$
 and it is irred / \mathbb{Q}
 by Eisenstein

$$\left. \begin{array}{l} f(x) = g(x+1) \\ f(x-1) = g(x) \end{array} \right\}$$

If $f(x)$ were reducible: $f(x) = a(x) b(x)$
 $g(x) = a(x-1) b(x-1)$ would be also reducible

$\Delta \Rightarrow g$ is reduc. so is f .

Cyclotomic polynomials

$x^n - 1$. We shall show how to factorise completely over \mathbb{Q}

First case: $x^p - 1$ p prime
 $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$

Define: $C_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ when p is prime

Prop. when p is prime
 $C_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ is irreducible over \mathbb{Q}

Proof $C_p(x) = \frac{x^p - 1}{x - 1}$

make change of variables $x = y + 1$

$$(y+1)^p = y^p + \sum_{i=1}^{p-1} \binom{p}{i} y^i + 1$$

$$\frac{(y+1)^p - 1}{y} = y^{p-1} + \sum_{r=1}^{p-1} \binom{p}{r+1} y^{r+1} = g(y)$$

then $g(y)$ satisfied Eisenstein

$$f_p(x) = g^{p-1}$$

So since g is irred/\mathbb{Q}
 $\therefore f_p$ is irred/\mathbb{Q}

Q.E.D.

Proof of Eisenstein Criterion

Stage 1:

If $a(x) = a_n x^n + \dots + a_1 x + a_0$ $a_i \in \mathbb{Z}$

$$a_n \not\equiv 0 \pmod{p}$$

$$a_r \equiv 0 \pmod{p} \quad 0 \leq r \leq n-1$$

$$a_0 \not\equiv 0 \pmod{p^2}$$

then $a(x)$ has no proper factorization over \mathbb{Z}

Proof of stage I:

Suppose $a(x) = b(x)c(x)$ is a proper factorisation over \mathbb{Z}
 i.e. $b(x) = b_m x^m + \dots + b_1 x + b_0$ $b_m \neq 0$
 $c(x) = c_k x^k + \dots + c_1 x + c_0$ $c_k \neq 0$
 and $m < n$ so $k < n$ $k+m = n$

First compare constant terms
 $a_0 = b_0 c_0$

$a_0 \equiv 0 \pmod{p}$ $a_0 \not\equiv 0 \pmod{p^2}$
 so either $p|b_0$ & $p \nmid c_0$ or
 $p|c_0$... $p \nmid b_0$

alog. same for others.

Next look at coeff of x .

$$a_1 = b_1 c_0 + b_0 c_1$$

$a_1 \equiv 0 \pmod{p}$ by hypothesis
 $b_0 \equiv 0 \pmod{p}$ by choice

so $b_1 c_0 \equiv 0 \pmod{p}$

But $c_0 \not\equiv 0 \pmod{p}$ so $b_1 \equiv 0 \pmod{p}$

Claim by induction each $b_r \equiv 0 \pmod{p}$
 can assume $b_0 \equiv 0 \pmod{p}$ // induction base
 $b_1 \equiv 0 \pmod{p}$

Suppose $b_r \equiv 0 \pmod{p}$ $r \leq r-1$

look at coeff. of x^r

$$a_r \equiv b_r c_0 + \sum_{t=0}^{r-1} b_t c_{r-t}$$

Inductively $\sum_{t=0}^{r-1} b_t c_{r-t} \equiv 0 \pmod{p}$

$$a_r \equiv 0 \pmod{p}$$

But $c_0 \not\equiv 0 \pmod{p}$ so $b_r \equiv 0 \pmod{p}$

so for each r $0 \leq r \leq m$ ($< n$)

$$b_r \equiv 0 \pmod{p}$$

$$\text{so } b_m \equiv 0 \pmod{p}$$

Compare coeffs of x^n

$$a_n = b_m c_n$$

$$\text{so } a_n \equiv 0 \pmod{p}$$

Contradiction: so $q(x)$ has no proper factorisation

Q.E.D.

Eisenstein's Lemma

If $a(x) \in \mathbb{Z}[x]$ has no proper factorization in \mathbb{Z} then $a(x)$ has no proper factorization in \mathbb{Q}

Def - n

Let $q(x) = a_n x^n + \dots + a_1 x + a_0$ $a_n \neq 0$
 whose $a_i \in \mathbb{Z}$
 By $c(q)$ we mean
 $c(q) = \text{HCF}(a_n, \dots, a_1, a_0)$ } Content of $q(x)$

Easy to see that if $r(x) \in \mathbb{Z}[x]$ can write
 $r(x) = c(r) q(x)$

where $q(x) \in \mathbb{Z}[x]$, $c(q) = 1$ \rightarrow then
 have out communal factors.

e.g. $r(x) = 6x^2 + 16x + 12$
 $= 6(x^2 + 16/6x + 12/6)$
 $= c(r) (q(x))$ | $c(r) = 6$

Prop. Gauss's Lemma

If $a(x), b(x) \in \mathbb{Z}[x]$, then $c(ab) = c(a)c(b)$

condition

Proof by above twice i.t.p.

if $c(a) = 1$ and $c(b) = 1$ then $c(ab) = 1$

So write $a(x) = a_n x^n + \dots + a_1 x + a_0$
 $b(x) = b_m x^m + \dots + b_1 x + b_0$

$c(ab) = 1 = c(b)$

$c(a) = 1 = c(b)$
 Must show that if p is a prime
 then there is at least one coeff of $a^r b^s$
 which p does not div.

Since $c(a) = 1$, choose v : $p \nmid a_v$ but
 $p \mid a_t$ for $t < v$

Since $c(b) = 1$ choose s : $p \nmid b_s$ but $p \mid b_t$ for $t < s$

coeff of x^{v+s} in $(a+b)^{v+s}$ look like

$$= a_v b_s + \sum_{t=1}^v a_t b_{v+s-t} + \sum_{t=1}^s a_{v+s-t} b_t$$

by choice $a_v b_s \not\equiv 0 \pmod p$,
 but $\sum_{t=1}^v a_t b_{v+s-t} \equiv 0 \pmod p$

and also
 $\sum_{t=1}^s a_{v+s-t} b_t \equiv 0 \pmod p$

coeff of a^{v+s} in $a(a) b(a)$ is $\not\equiv 0 \pmod p$

$c(a, b) = 1$ Q.E.D.

23/03/11

Proof of collatz conjecture - gauss's lemma

write $a(b) b(a) = c(x)$, where $c(x) = 1$

So $c = (a, b)$

write $a(a) = c_1 a_1(a)$

$$c(\tilde{a}) = c(\tilde{a}) = 1$$

$$a(x)b(x) = c_1 c_2 \tilde{a}(x) \tilde{b}(x)$$

but $c(\tilde{a}\tilde{b}) = 1$

Compare $\begin{cases} a(x)b(x) = c_1 c_2 \tilde{a}(x) \tilde{b}(x) \\ a(x)b(x) = c \tilde{a} \tilde{b} \end{cases} \Rightarrow c = c_1 c_2$

Q.E.D.

Corollary if $p(x) \in \mathbb{Z}[x]$ $\deg(p) = n$
 suppose $p(x) = \alpha(x)\beta(x)$
 $\alpha(x), \beta(x) \in \mathbb{Q}[x], \deg \alpha = m, \deg \beta = k$
 $m+k = n$
 then $p(x) = a(x)b(x)$, where $a(x), b(x) \in \mathbb{Z}[x]$,
 $\deg a(x) = \deg \alpha = m, \deg b(x) = \deg \beta = k$

Proof:

Assume $c(p) = 1$

clear factors in α, β and write $A(x) = D\alpha(x)$

$$B(x) = D'\beta(x)$$

where D, D' non-zero integers; $A(x), B(x) \in \mathbb{Z}[x]$

$$\therefore DD'p(x) = A(x)B(x)$$

write $c = c(A) \quad c' = c(B)$

$$\text{so } A(x) = c a(x) \quad c(a) = 1$$

$$B(x) = c' b(x) \quad c(b) = 1$$

and $a, b \in \mathbb{Z}[x]$

$$BD'p(x) = cc' a(x)b(x)$$

$DD' = \text{content LHS}$

$$DD' = cc'$$

$cc' = \text{content RHS}$

so $p(x) = \alpha(x)\beta(x)$ as claimed

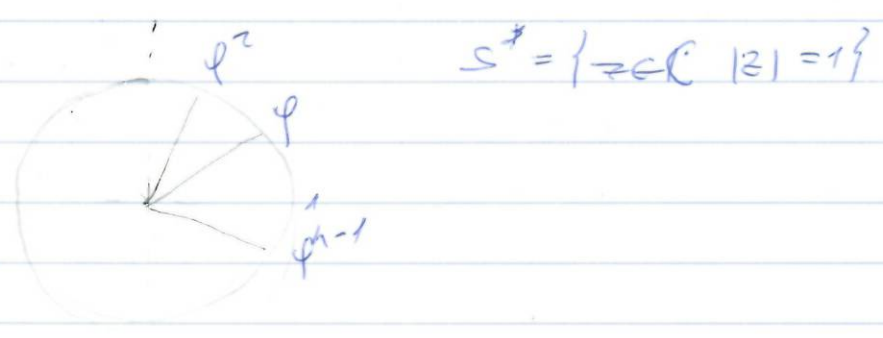
If $c(p) > 1$, then write $f(x) = c(p) \tilde{p}(x)$
 $c(\tilde{p}) = 1$
 $\tilde{p}(x) = \frac{f(x)}{c(p)}$

(if proceed as above) **QED**

Corollary If $f(x) \in \mathbb{Z}[x]$ then $f(x)$ has no proper factorization **called π**
 iff $f(x)$ has no proper factorisation / \mathbb{Q}

Corollary If $f(x) \in \mathbb{Z}[x]$ satisfies Eisenstein then **it is $\text{irred} / \mathbb{Q}$**

Application: How to factorise $x^n - 1$ completely / \mathbb{Q}
 over \mathbb{C} : Take $\zeta_n = \exp\left(\frac{2\pi i}{n}\right) = \zeta$
 So $x^n - 1 = (x-1)(x-\zeta)(x-\zeta^2) \dots (x-\zeta^{n-1})$



Obviously $\text{ord}(\zeta_n^d)$ divide n
 let d be a divisor of n
 define $\varphi(x) = \prod_{\text{ord}(\zeta_n^r) = d} (x - \zeta_n^r)$

It turns out that each $c_d(x) \in \mathbb{Z}[x]$
and $c_d(x) \notin \mathbb{Q}$

So now: $x^n - 1 = \prod_{d|n} c_d(x)$

So let's go!! $x-1 = c_1(x)$

$x^2 - 1 = (x-1)(x+1)$

$x^2 - 1 = c_1(x) c_2(x)$

So $c_2(x) = x+1$

$x^3 - 1 = c_1(x) c_3(x)$

$= (x-1)(x^2+x+1)$

$x^4 - 1 = c_1(x) c_2(x) c_4(x)$

$= (x-1)(x+1) c_4(x)$

$= (x^2-1)(x^2+1)$

$c_5 = \frac{x^5-1}{x-1} = c_1(x) c_5(x)$

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

$x^6 - 1 = c_1(x) c_2(x) c_3(x) c_6(x)$

$= (x^3-1)(x+1) c_6(x)$

$= (x^4+x^3-x-1) c_6(x)$

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

$= (x^3-1)(x+1)(x^2-x+1)$

$x^7 - 1 = c_1(x) c_7(x)$

$= (x-1) c_7(x)$

$x^8 - 1 = c_1 c_2 c_4 c_8$

$= (x^4-1) c_8$

$x^9 - 1 = c_1 c_3 c_9$

$= (x^3-1) c_9$

solar \Rightarrow

$c_1(x) = x-1$

$c_2(x) = x+1$

$c_3(x) = x^2+x+1$

$c_4(x) = x^2+1$

$c_5(x) = x^4+x^3+x^2+x+1$

$c_6(x) = x^2-x+1$

$c_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$

$c_8(x) =$

$c_9(x) =$

$c_{10}(x) =$

$c_{11}(x) =$

$= (x+1) c_{10}$

$c_{12}(x) =$

Give complete factorization $x^5 - 1 / \mathbb{Q}$

$$\begin{aligned}
 x^{15} - 1 &= C_1 C_2 C_3 C_6 C_9 C_{18} \\
 &= (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^2+1) C_{18} \\
 &= (x^6-1)(x^6+x^3+1) C_{18} \\
 &= (x^6-1)(x^6+x^3+1)(x^6-x^3+1)
 \end{aligned}$$

$$\frac{x^{15}-1}{x^6-1} = x^9 + x^3 + 1$$

$$\frac{y^3-1}{y-1} = y^2 + y + 1$$

So $C_{18}(x) = \left(\frac{x^{12} + x^6 + 1}{x^6 + x^3 + 1} \right) = x^6 - x^3 + 1$

$$\begin{array}{r}
 x^6 - x^3 + 1 \\
 \hline
 x^6 + x^3 + 1 \quad \left. \begin{array}{l} x^6 \\ x^3 \\ 1 \end{array} \right\} \begin{array}{l} x^6 \\ x^3 \\ 1 \end{array} \\
 \hline
 x^{12} \quad x^6 \quad 1 \\
 \hline
 x^{12} + x^9 + x^6 \\
 \hline
 -x^9 + 1 \\
 \hline
 -x^9 + x^6 - x^3 \\
 \hline
 x^6 + x^3 + 1
 \end{array}$$

$x^2 + 1$?

$$\begin{aligned}
 &(x^{2n}-1)(x^n-1)(x^n+1) \\
 \left(\frac{x^{2n}-1}{x^n-1} \right) &= x^n + 1 \quad \text{new factors } \frac{x^{2n}-1}{x^n-1}
 \end{aligned}$$

& card