7202 Algebra 4: Groups and Rings Notes

Based on the 2011-2012 lectures by Prof F E A Johnson

Algebra 4 : Remember : Get to know examples. 10th Jan 2012

A group G consists of 3 things

$$G = (G, *, e)$$

1) G is a set
2) $e \in G$ $(G \neq \emptyset)$
3) $* : G \times G \to G$ is a mapping $*(g,h) = g*h$ such that
4) $g*(h*k) = (g*h)*k$ ASSOC
5) $g*e = e*g = g$ IDENTITY
6) $\forall g \in G \; \exists g^{-1} \in G$ st $g*g^{-1} = e = g^{-1}*g$ INVERSES.

$$(g*h)^{-1} = h^{-1}*g^{-1}$$

We rarely use this notation.

TWO MAIN CONVENTIONS

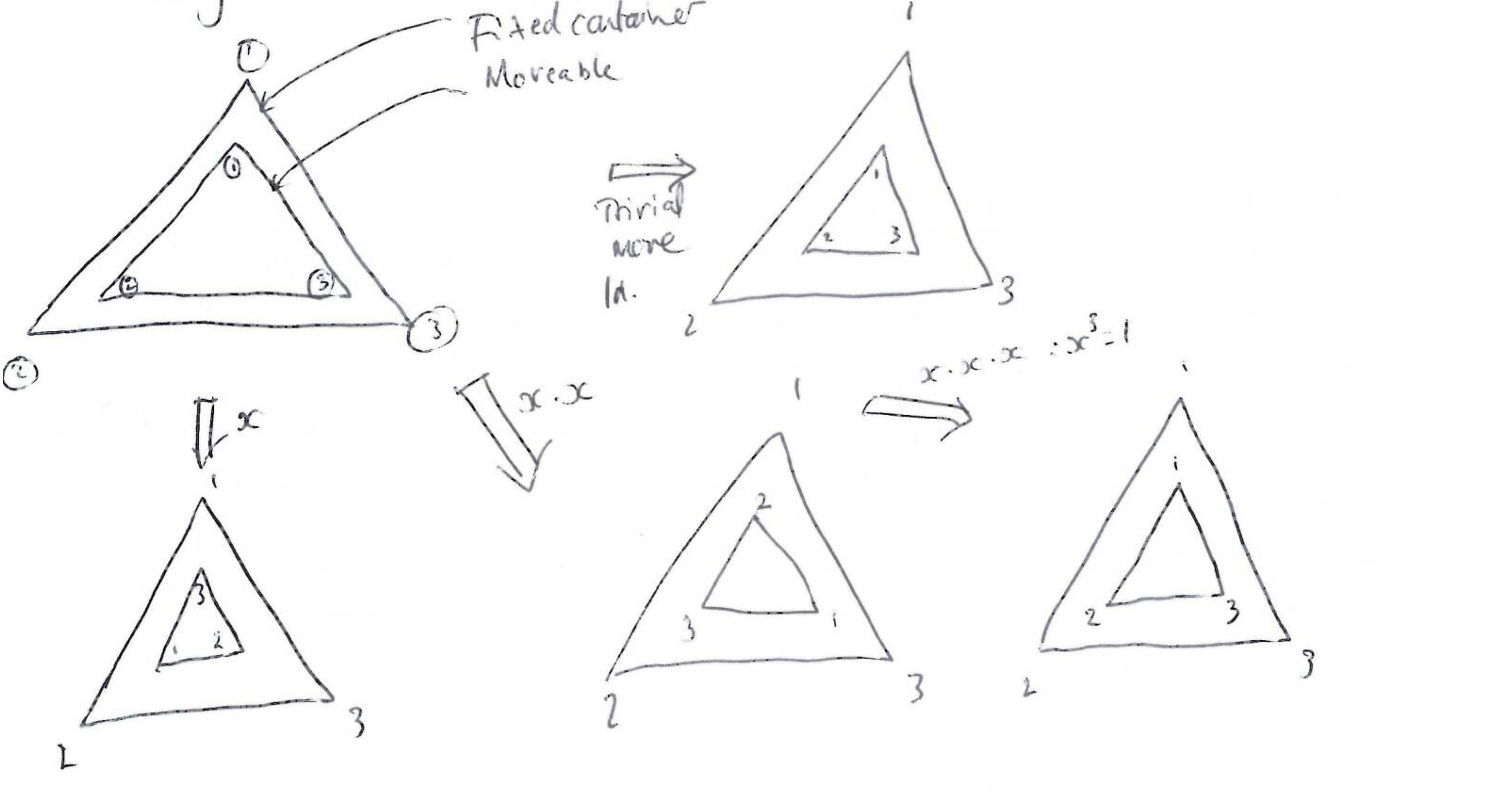
I) Multiplicative convention : $\cdot$ instead of $*$, 1 instead of e

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

II) Additive convention : $+$ instead of $*$, 0 instead of e, $-g$ instead of g^{-1}

$g+0 = 0+g = g$ $\quad$ ~~$g+g^{-1} = g^{-1}+g$~~ $= 0 = g+(-g) = (-g)+g$

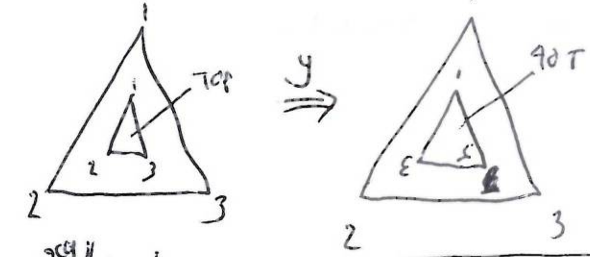
Only ever used when we also have $g+h = h+g$ $\forall g,h \in G$. Commutati



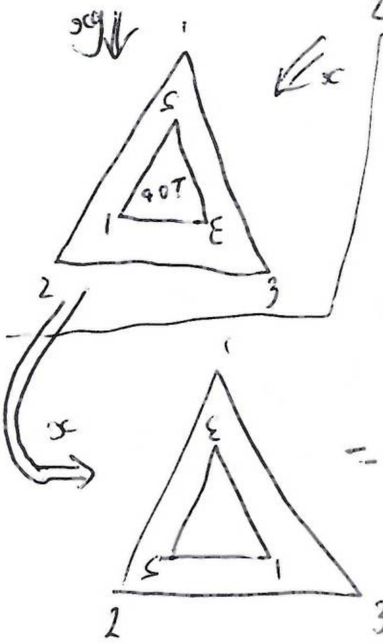
C_3 : Symmetry of 1sided equilatral triangle.

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	$x^3=1$
x^2	x^2	1	x

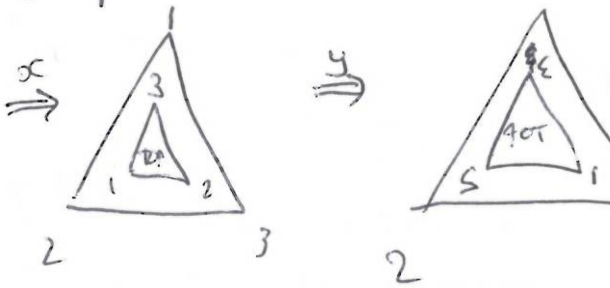
Symmetries of 2 sided equil Δ.



Compose in functional order
$x \cdot y$ = first y then x



Compose : First x then y.



$= yx$

$yx \neq xy$

$= x^2 y$

so $\quad yx = x^2 y$

First eg of a nonabelian group (ie noncommutative)
D6 , dihedral group of order 6.

D6

$\cdot$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	$\bigcirc\!\!\!\!\!\;xy$	1	x^2	x
xy	xy	y	x^2y	x	$\textcircled{1}$	x^2
x^2y	x^2y	xy	y	x^2	x	$\textcircled{1}$

left first.

$\rightarrow yx^2 = (x^2y)x = x^2(yx)$
$= x^2(x^2y) = x^4y = xy$

$\rightarrow (xy)(xy) = x(yx)y = x(x^2y)y$
$= x^3y^2 = 1 \cdot 1 = 1$

$\rightarrow (x^2y)(x^2y) = x^2(yx^2)y$
$= x^2(xy)y = x^3y^2 = 1$

(eg) Q_8 quaternion group of order 8

$i^2 = -1$ $a+ib$ is 2 dimensional

Take $i^2 = -1$ $j^2 = -1$ $k^2 = -1$

$a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$ $a, b, c, d \in \mathbb{R}$.

$ij = k = -ji$

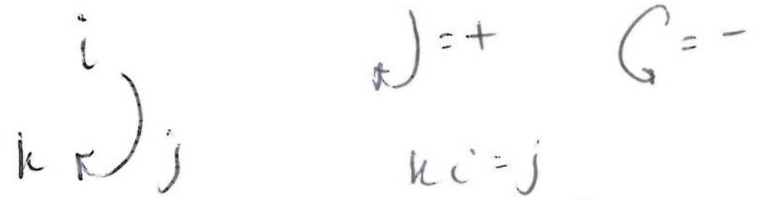
	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	$\bigcirc\!\!\!\!-j$	$\bigcirc\!\!\!\!j$
-i	-i	i	1	-1	-k	k	+j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k						
-k	-k	k						

$ik = i \cdot ij = i^2 j = -j$

~~$j = -ik$~~

~~$ji =$~~

... Finish off.



$ki = j$

$ik = -j$

$\Rightarrow$ Finished corner:

j	-j	-i	i	-1	1
-j	j	i	-i	1	-1

Algebra

13th Jan 2012

Lec: 9 → 11 Tues Archaeology
PC: 11 → 12 Bedford Way LG04 } Fri
Lec 12 → 1 Chem LT.

So far we know

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

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

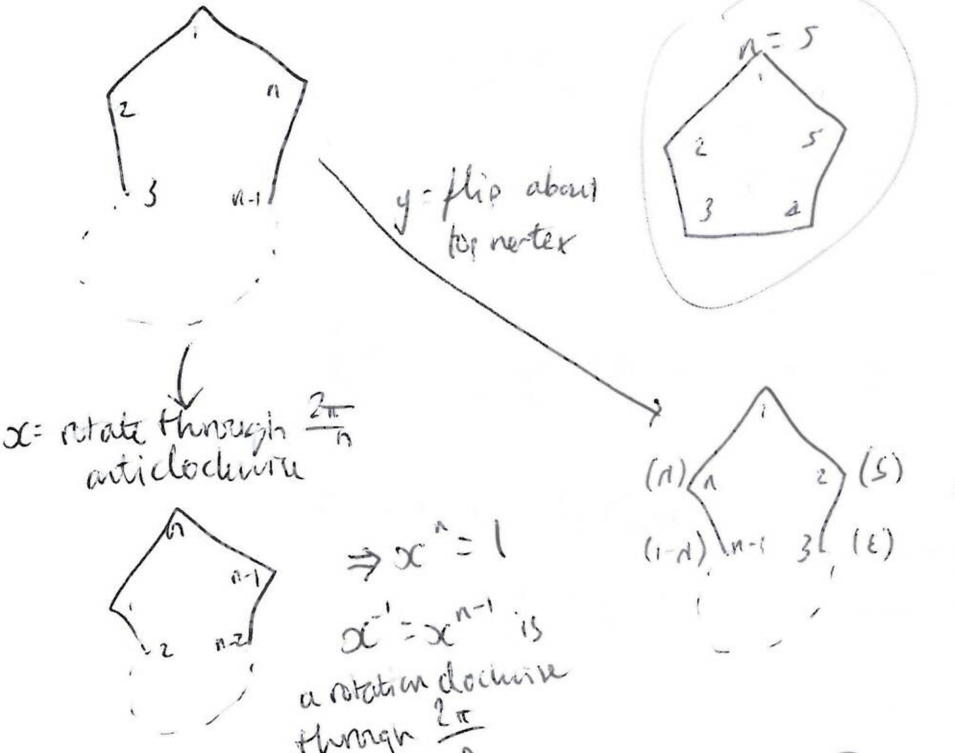
$Q_8 = \{1, -1, i, -i, j, -j, k, -k \mid i^2 = j^2 = k^2 = -1, ij = k = -ji\}$

It follows that $jk = -kj = i$, $ki = -ik = j$

Generalisation of C_3: C_n; symmetries of 1-sided regular n-gon.

Algebraically; $C_n = \{1, x \ldots x^{n-1} \mid x^n = 1\}$ Cyclic group of order n.

Generalisation of D6: D_{2n}; the symmetries of 2-sided regular n-gon.

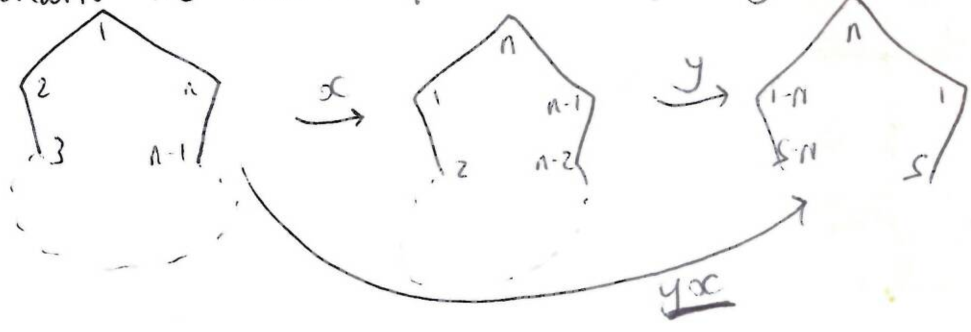


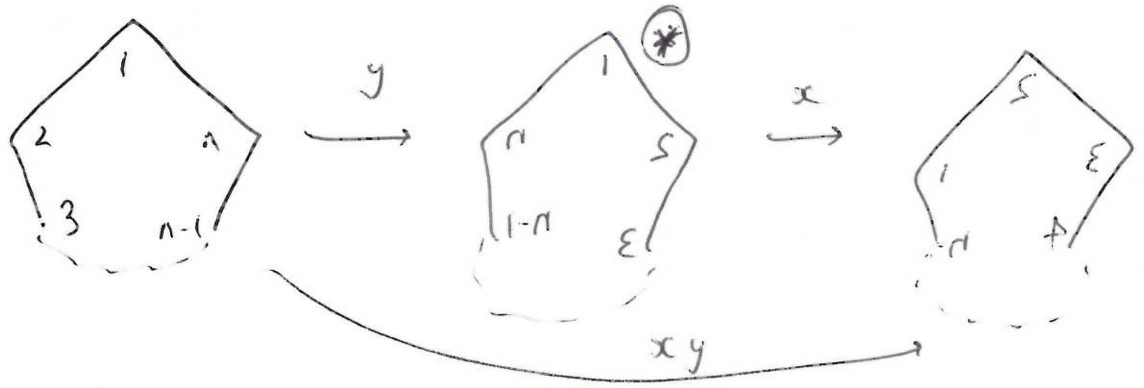
⇒ $x^n = 1$

$x^{-1} = x^{n-1}$ is a rotation clockwise through $\frac{2\pi}{n}$

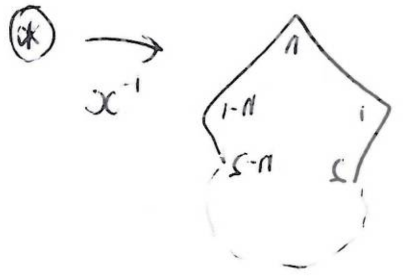
⇒ $y^2 = 1$

What is the relationship between yx, xy?





clearly, $yx \neq xy$



$\Rightarrow x^{-1}y = yx$

$x^{n-1}y = yx$

Write D_{2n} algebraicly as follows;

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

Note: $yx^2 = ?$ $(yx)x = x^{n-1}yx = x^{n-1}x^{n-1}y = x^{2n-2}y$

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

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

Compare D_8 with Q_8 (both non abelian of order 8)

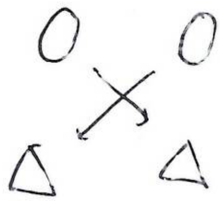
D_8	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	1	x^3	x^2	x
xy	xy	y	x^3y	x^2y		1		
x^2y	x^2y	xy	y	x^3y			1	
x^3y	x^3y	x^2y	xy	y				1

← fill in.

$(xy)(xy) = x(yx)y = x(x^3y)y$
$= x^4y^2 = 1$

Q_8	1	-1	i	-i	j	-j	k	-k
1	1							
-1		1						
i			-1					
-i				-1				
j					-1			
-j						-1		
k							-1	
-k								-1

What does it mean for two groups to be "the same" or "different"?



Say that two sets A, B are "essentially the same" when $\exists$ a bijective mapping

$$\varphi : A \xrightarrow{\simeq} B$$

<u>Defn</u>: Let G, H be groups. By a ~~group~~ homomorphism $\varphi : G \longrightarrow H$, I mean a mapping such that

$\varphi(x,y) = \varphi(x)\varphi(y)$ $\forall x, y \in G$ ie it takes a product to a product

It preserves multiplication.

We say that G is isomorphic to H when $\exists$ bijective homomorphism $\varphi : G \to H$.

<u>Formal consequences of defn</u>:

Let $\varphi : G \longrightarrow H$ be a homo; then

<u>Prop</u>: $\varphi(1_G) = 1_H$ ie φ preserves identities.

<u>Proof</u>: $1_G 1_G = 1_G$. Apply φ. $\varphi(1_G 1_G) = \varphi(1_G)$

$$\downarrow$$

$$\varphi(1_G)\varphi(1_G) = \varphi(1_G)$$

Multiply on the right by $\varphi(1_G)^{-1}$ ($\in H$)

$$\varphi(1_G)[\varphi(1_G)\varphi(1_G)^{-1}] = \varphi(1_G)\varphi(1_G)^{-1} = 1_H$$

$$\varphi(1_G)1_H = 1_H \implies \varphi(1_G) = 1_H \quad \text{QED.}$$

__Prop__: $\forall g \in G \quad \varphi(g^{-1}) = \varphi(g)^{-1}$

__Proof__: $g^{-1}g = 1_G$ so apply φ

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

Multiply on right by $\varphi(g)^{-1}$

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

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

Group homos do occur in other parts of Mathematics

__1st example__:

$$\exp : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}_{>0}, \cdot, 1)$$

$$\exp(x+y) = \exp(x)\exp(y)$$

$$\exp(0) = 1$$

$$\exp(-x) = \exp(x)^{-1}$$

Inverse: Isomorphism is

$$\log : (\mathbb{R}, \cdot, 1) \longrightarrow (\mathbb{R}, +, 0)$$

$$\log(x) = \int^{x} \frac{dt}{t}$$

$$\log(xy) = \log(x) + \log(y)$$

$$\log(1) = 0$$

$$\log\left(\frac{1}{x}\right) = -\log(x)$$

We think of isomorphic groups as being "the same", and non isomorphic groups as being different.

(eg) $C_2 = \{1, x\} \quad x^2 = 1$

$\mathbb{F}_2 = \{0, 1\} \quad 1 + 1 = 0$

$$\left.\begin{array}{l}\varphi(1) = 0 \\ \varphi(x) = 1\end{array}\right\} \text{ like log}$$

$\cdot C_2$	1	x
1	1	x
x	x	1

$\mathbb{F}_2 +$	0	1
0	0	1
1	1	0

Naive proposition but "good enough" for now.

Prop: Let $\varphi : G \to H$ be a group $\boxed{\text{isomorphism}}$

ie. $G \cong H$ or $G \overset{\varphi}{\cong} H$ ← G isomorphic by φ to H.

Let $\mathcal{Y}(G) = \{x \in G \, ; \, x^2 = 1\}$ $x^2 = 1 \iff x^{-1} = x$

$\mathcal{Y}(H) = \{y \in H \, ; \, y^2 = 1\}$ Then $\varphi : \mathcal{Y}(G) \to \mathcal{Y}(H)$ is bijective

Proof: Since φ preserves products, $\varphi(x^2) = \varphi(x)^2$

If $x^2 = 1$ $\varphi(x^2) = \varphi(1) = 1$ so $\varphi(x)^2 = 1$

ie if $x \in \mathcal{Y}(G)$ then $\varphi(x) \in \mathcal{Y}(H)$

Because $\varphi : G \to H$ is injective. then

$\varphi : \mathcal{Y}(G) \to \mathcal{Y}(H)$ is also injective

Suppose $y \in \mathcal{Y}(H)$ $y^2 = 1$

Choose $x \in G$ $\varphi(x) = y$, φ surjective. claim $x^2 = 1$

$\varphi(x^2) = \varphi(x)^2 = y^2 = 1$

But also $\varphi(1) = 1$

But φ injective so $x^2 = 1$ so $\forall y \in \mathcal{Y}(H)$ $\exists x \in \mathcal{Y}(G)$

st $\varphi(x) = y$

So $\varphi : \mathcal{Y}(G) \to \mathcal{Y}(H)$ is bijective as claimed. QED.

Corollary: $D_8 \not\cong Q_8$

Pf: Wrote out multiplication tables: We saw

$\mathcal{Y}(D_8) = \{1, x^2, y, xy, x^2y, x^3y)$ has 6 elements only

$\mathcal{Y}(Q_8) = \{1, -1\}$ has 2 elements. QED.

General advice:

To show two groups are isomorphic, we need to construct a mapping $\varphi : G \to H$, bijective & homo.

To show two groups are NOT isomorphic we need to produce an invariant

⑪ Permutation groups

$\sigma_n = \{\sigma : \{1 \ldots n\} \to \{1 \ldots n\}\}$ σ is a bijective mapping

Define group operation to be composition $|\sigma_n| = n!$

$\sigma_2, \sigma_3, \sigma_4, \sigma_5 \ldots$

$2 \quad 6 \quad 24 \quad 120 \ldots$

$$\sigma_2 = \left\{ \underset{id}{\underset{\shortparallel}{\begin{pmatrix}1&2\\1&2\end{pmatrix}}} \ \underset{\tau}{\underset{\shortparallel}{\begin{pmatrix}1&2\\2&1\end{pmatrix}}} \right\} \qquad \tau^2 = Id \qquad \sigma_2 \cong C_2$$

	1	τ
1	1	τ
τ	τ	1

$$\sigma_3 = \left\{ \overset{1}{\overset{\shortparallel}{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}}} \overset{x}{\overset{\shortparallel}{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}}} \overset{x^2}{\overset{\shortparallel}{\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}}} \underset{Y}{\underset{\shortparallel}{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}}} \right.$$

$$\left. \underset{xY}{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}} \underset{x^2Y}{\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}} \right\}$$

$$x^2 = \left| \begin{matrix}1&2&3\\2&3&1\\3&1&2\end{matrix} \right| \begin{matrix}\}x\\ x^3=1\end{matrix} \qquad Y^2 = \begin{pmatrix}1&2&3\\3&2&1\\1&2&3\end{pmatrix} \quad Y^2 = 1.$$

$$YX = \begin{pmatrix}1&2&3\\2&3&1\\ \\1&3&2\end{pmatrix} \begin{matrix}\}x\\ \}Y\end{matrix} \qquad xY = \xcancel{\begin{matrix}1&2&3\\3&2&1\\1&3&2\end{matrix}} \quad \begin{pmatrix}1&2&3\\2&1&3\\3&2&1\end{pmatrix} \}Y$$

so $YX = x^2Y$

so $\sigma_3 \cong D_6$ explicitly.

$1 \to 1$
$x \to x$
$x^2 \to x^2$
$Y \to Y$
$xY \to xY$
$x^2Y \to x^2Y$

$x^3 = 1 \quad x^3 = 1$
$Y^2 = 1 \quad Y^2 = 1$
$YX = x^2Y \quad YX = x^2Y$

Algebra 17th Jan 2012

G group, $g \in G$ By convention.

$\text{ord}(g) = \min\{r \geq 1 : g^r = 1\}$ $g^0 = 1$

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

$\text{ord}(x) = 12$ $(\text{ord}(1) = 1)$

$(x^2)^6 = 1$ $x^2, x^4, x^6, x^8, x^{10}, x^{12}$ x^5

$\text{ord}(x^2) = 6$

$\text{ord}\, x^3 = 4$ $x^6 = 2$ $x^9 = 4$

$x^4 = 3$ $x^7 = 12$ $x^{10} = 6$

$x^5 = 12$ $x^8 = 3$ $x^{11} = 12$

Thm: In $C_n = \{1, x, \ldots x^{n-1}\}$

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

Prop: In $C_n = \{1, x, \ldots, x^{n-1}\}$ If $x^N = 1$ and $1 \leq N$ then $N = nq$ for some q (ie N is a multiple of n)

Proof: Suppose $x^N = 1$ & $1 \leq N$

Either $\underset{(i)}{1 \leq N < n}$ or $\underset{(ii)}{N = n}$ or $\underset{(iii)}{n < N}$

(i) can't occur because it contradicts contradiction as n is $\min\{r \geq 1, x^r = 1\}$

(ii) Take $q = 1$

(iii) Write $N = qn + r$, $0 \leq r \leq n-1$

$1 = x^N = x^{qn+r} = (x^{n\cancel{q}})^q x^r$ But $x^n = 1$ so I get

$x^r = 1$ ~~in~~ where $0 \leq r \leq n-1$. If $r \neq 0$ get $\times$ again so

$r = 0 \Rightarrow N = nq$ □.

Thm: In $C_n = \{1, x, \ldots, x^{n-1}\}$ $\text{ord}\, x^a = \frac{n}{\text{HCM}(n,a)}$ $[1 \leq a \leq n-1]$

Proof: Suppose $\text{ord}(x^a) = k$ $\Rightarrow (x^a)^k = 1$ by defn.

So $x^{ak} = 1$. By previous result, ak is a multiple of n

ak is obviously a multiple of a. So ak is a common multiple of a, n. But $k = \min\{r \geq 1 : (x^a)^r = 1\}$ Since a is fixed ak = lowest common multiple of a, n $\Rightarrow$ k is minimised

$$ak = LCM(a,n) = \frac{an}{HCF(a,n)}$$

$$\Rightarrow k = \frac{n}{HCF(n,a)} \quad \square.$$

Question: $C_n = \{1, x, \dots, x^{n-1} \mid x^n = 1\}$ When is $ord(x^a) = n$?

when a, n have no common factor except 1 (coprime)

Look at C_{12} again...

$C_{12} = \{1, x, \dots x^{11} \mid x^{12} = 1\}$ x generates C_{12}

Every other element is a power of x

x^2 doesn't generate C_{12} $\to 1, x^2, x^4, x^6, x^8, x^{10}, x^{12}, 1, x^2, x^4 \dots$ no odds.

x^a generates C_{12} iff $ord(x^a) = 12$

so... x, x^5, x^7, x^{11}, all generate C_{12}.

no other elements generate C_{12}

Generalisation:

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

x^a generates C_n $\boxed{\text{iff}}$ $ord(x^a) = n$ $\boxed{\text{iff}}$ a, n coprime

Homomorphisms $C_n \longrightarrow C_n$:

$\varphi : C_n \to C_n$ such that $\varphi(gh) = \varphi(g)\varphi(h)$ $\forall g, h$

$\varphi(x^s x^t) = \varphi(x^s)\varphi(x^t)$ However, $\varphi(x^s) = \varphi(x x^{s-1})$

$= \varphi(x)\varphi(x^{s-1}) = \dots = \varphi(x)^s$

Prop: A homomorphism $\varphi : C_n \to C_n$ is completely determined by $\varphi(x)$ where x is a generator of C_n.

Proof: $C_n = \{1, x, \dots, x^{n-1} / x^n = 1\}$ if I want to calculate $\varphi(x^s)$ then $\varphi(x^s) = \varphi(x)^s$ ie $\varphi(x)$ determines $\varphi(g)$ $\forall g \in C_n$. D.

m: $C_n = \{1, x, \ldots, x^{n-1} / x^n = 1\}$

Let $0 \leq a \leq n-1$. Define $\varphi_a : C_n \to C_n$ by

$\varphi_a(x) = x^a$, so $\varphi_a(x^s) = x^{as} = (x^a)^s$

φ_a is a homomorphism. Why?

$$\varphi_a(x^s x^t) = \varphi_a(x^{s+t}) = x^{a(s+t)} = x^{as} x^{at} = \varphi_a(x^s)\varphi_a(x^t)$$

Corollary: Every homomorphism $\varphi : C_n \to C_n$ is of form $\varphi = \varphi_a$ for some a: ~~constant~~ $0 \leq a \leq n-1$.

Proof: $\varphi(x) \in \{1, x, \ldots, x^{n-1}\}$

Suppose $\varphi(x) = x^a$ $\quad \varphi(x^s) = (x^a)^s = x^{as} = \varphi_a(x^s)$

ie $\varphi = \varphi_a$ $\quad \square$

So there are exactly n homomorphisms, $C_n \to C_n$.

(eg) Homomorphisms $C_3 \to C_3$ $\qquad C_3 = \{1, x, x^2 / x^3 = 1\}$

$\varphi_0 : C_3 \to C_3$ $\qquad \varphi_0(x) = x^0 = 1$

So $\varphi_0(1) = 1$, $\varphi_0(x) = 1$, $\varphi_0(x^2) = \varphi_0(x)^2 = 1^2 = 1$

So φ_0 is very boring. $\varphi_0(x^a) = 1$ $\forall a$. Trivial homo.

$\varphi_1 : C_3 \to C_3$ $\qquad \varphi_1(x) = x$

$\varphi_1(x^2) = \varphi_1(x)\varphi_1(x) = xx = x^2$, $\varphi_1(1) = 1$ (homo)

$\varphi_1(1) = 1$ $\quad \varphi_1(x) = x$, $\varphi_1(x^2) = x^2$ so $\varphi_1 = \text{Id}$ homo.

$\varphi_2 : C_3 \to C_3$ $\qquad \varphi_2(x) = x^2$

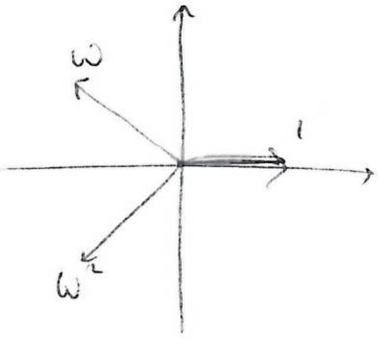
$\varphi_2(x^2) = \varphi_2(x)\varphi_2(x) = x^2 x^2 = x^4 = x$

$\varphi_2(1) = \varphi_2(x \cdot x^2) = \varphi_2(x)\varphi_2(x^2) = x^2 . x = x^3 = 1$

because φ_1 is homo.

$\varphi_2(1) = 1$ $\quad \varphi_2(x) = x^2$ $\quad \varphi_2(x^2) = x$

This is familiar from complex analysis.



$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ so $\omega \to \omega^2$ is complex conjugate

$(1, \omega, \omega^2) \simeq C_3$

G, H groups, an isomorphism $\varphi: G \to H$ is a bijective homo

Special case: $H = G$

A bijective homo $\varphi: G \to G$ is called an automorphism of G. We'll determine all automorphisms of C_n

Let G be a group. Define:

$Aut(G) \{\alpha : G \to G : \alpha$ is an automorphism$\}$

ie α is bijective and a homo.

<u>Prop</u>: If $\alpha, \beta \in Aut(G)$ then $\alpha \circ \beta \in Aut(G)$

ie the composition of two autos is an auto.

<u>Proof</u>: $\alpha \circ \beta : G \to G$ is a homo because if $x, y \in G$

then $(\alpha \circ \beta)(xy) = \alpha(\beta(xy)) = \alpha(\beta(x)\beta(y))$

$= \alpha[\beta(x)]\,\alpha[\beta(y)] = (\alpha \circ \beta)(x)(\alpha \circ \beta)(y)$

$\alpha \circ \beta$ is bijective because the composition of any two bijections is a bijection $\square$.

Got "operation"

$\circ : Aut(G) \times Aut(G) \to Aut(G)$

$(\alpha \times \beta) \longrightarrow \alpha \circ \beta$

<u>Prop</u>: $Aut(G)$ is a group with respect to the above product.

<u>Proof</u>: Composition is always associative so no problem with associative axiom. Take $1 = Id_G : G \to G$

$Id_G(x) = x \ \forall x \in G$. Clear that $Id_G \in Aut(G)$.

$Id_G(xy) = xy = Id_G(x)\, Id_G(y)$.

$\alpha \circ Id_G = \alpha = Id_G \circ \alpha$ so Id_G is an IDENTITY for $Aut(G)$

Inverses? Let $\alpha \in Aut(G)$. α is a bijective homo.

Because α is bijective, there is an inverse mapping.

$\alpha^{-1}: G \to G$ $\qquad \alpha \circ \alpha^{-1} = Id_G = \alpha^{-1} \circ \alpha$

Need to show α^{-1} is a homo.

Compare $\alpha^{-1}(xy)$ with $\alpha^{-1}(x)\alpha^{-1}(y)$

Apply α to each. $\alpha\alpha^{-1}(xy) = xy$ (Defn of α^{-1})

$\alpha[\alpha^{-1}(x)\alpha^{-1}(y)] = \alpha\alpha^{-1}(x)\,\alpha\alpha^{-1}(y)$ because α is homo.

$= xy$ again by defn of α^{-1}.

So. $\alpha[\alpha^{-1}(xy)] = xy = \alpha[\alpha^{-1}(x)\alpha^{-1}(y)]$

But α is injective so $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$.

and α^{-1} is a homo □.

So given a group G we've produced another group Aut(G

(eg) Aut(C_3) - Significant eg.

There are 3 homos : $C_3 \to C_3$

$$\begin{array}{lll} & & \tau \\ \varphi_0(1) = 1 & \varphi_1(1) = 1 & \varphi_2(1) = 1 \\ \varphi_0(x) = 1 & \varphi_1(x) = x & \varphi_2(x) = x^2 \\ \varphi_0(x^2) = 1 & \varphi_2(x^2) = x^2 & \varphi_2(x^2) = x \\ & \text{Id} & \end{array}$$

Of these three homos only two are autos, namely $\varphi_1 = Id$ and $\varphi_2 = \tau$

Aut(C_3)	1	τ
1	1	τ
τ	τ	1

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

$(\tau \circ \tau)(x) = \tau(\tau(x)) = \varphi_2(\varphi_2(x)) = \varphi_2(x^2)$

$= \varphi_2(x)^2 = (x^2)^2 = x^4 = x$ $\quad$ so $\tau \circ \tau = 1$

Aut $C_3 \cong C_2$

(eg) Aut(C_5) $\quad C_5 = \{1, x, x^2, x^3, x^4 \mid x^5 = 1\}$

There are 5 homos : $\alpha: C_5 \to C_5$

$\alpha \in \{\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4\}$

$\varphi_0(x^r) = 1$ isn't injective. $\varphi_1 = Id.$

$\varphi_1(1) = 1$
$\varphi_1(x) = x$
$\varphi_1(x^2) = x^2$
$\varphi_1(x^3) = x^3$
$\varphi_1(x^4) = x^4$

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

$\varphi_3(1) = 1$
$\varphi_3(x) = x^3$
$\varphi_3(x^2) = x$
$\varphi_3(x^3) = x^4$
$\varphi_3(x^4) = x^2$

$\varphi_4(1) = 1$
$\varphi_4(x^{1}) = x^4$
$\varphi_4(x^2) = x^3$
$\varphi_4(x^3) = x^2$
$\varphi_4(x^4) = x$

---

all bijective. So $Aut\, C_5 = \varphi_1, \varphi_2, \varphi_3, \varphi_4 \}$ is a group of order 4

Put $\alpha = \varphi_2$

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

  $\alpha^2(x) = x^4$ so $\alpha^2 = \varphi_4$

- $\alpha^3(x) = \alpha(\alpha^2(x)) = \varphi_2(x^4) = x^8 = x^3$

  $\alpha^3(x) = x^3$ so $\alpha^3 = \varphi_3$

- $\alpha^4(x) = \alpha(\alpha^3(x)) = \varphi_2(x^3) = x^6 = x$

  $\alpha^4(x) = \varphi_1 = Id.$

SO $Aut(C_5) = \{1, \alpha, \alpha^2, \alpha^3 \mid \alpha^4 = 1\}$ where I'm taking

$\alpha = \varphi_2 : C_5 \to C_5$, $\alpha(x) = x^2$

$Aut(C_5) \cong C_4$

So far: $Aut\, C_3 \cong C_2$
$Aut\, C_5 \cong C_4$

$\underset{\sim\sim}{Aut\, C_6}$ First make a general obrerration

<u>Thm</u>: Let $0 \leq a \leq n-1$ $\varphi_a : C_n \to C_n$ is an auto iff a is coprime to n

$C_6 = \{1, x, x^2, x^3, x^4, x^5 \mid x^6 = 1\}$ look at $\varphi_a : 0 \leq a \leq 5$

φ_0 is never injective so not an auto

$\varphi_1 = Id$ is always an auto

$\varphi_2 = ?$ . . .

$$\left.\begin{array}{l}\varphi_2(1)=1\\ \varphi_2(x)=x^2\\ \varphi_2(x^2)=x^4\\ \varphi_2(x^3)=x^6=1\end{array}\right\} \rightarrow$$ so φ_2 not injective $\varphi_2(1)=\varphi_2(x^3)$ $x^3 \neq 1$

$\varphi_3(1)=\varphi_3(x^2)$ $1 \neq x^2$ not injective. $\leftarrow \left\{\begin{array}{l}\varphi_3(1)=1\\ \varphi_3(x)=x^3\\ \varphi_3(x^2)=1\end{array}\right.$

$$\left.\begin{array}{l}\varphi_4(1)=1\\ \varphi_4(x)=x^4\\ \varphi_4(x^2)=x^2\\ \varphi_4(x^3)=1\end{array}\right\} \text{no.}$$

$$\left.\begin{array}{l}\varphi_5(1)=1\\ \varphi_5(x)=x^5\\ \varphi_5(x^2)=x^4\\ \varphi_5(x^3)=x^3\\ \varphi_5(x^4)=x^2\\ \varphi_5(x^5)=x\end{array}\right\}$$ φ_5 is bijective $\Rightarrow$ auto.

$\mathrm{Aut}(C_6)=\{1,\varphi_5\}$ $\varphi_5^2=1$

$\mathrm{Aut}(C_6)\cong C_2$

Proof of Thm: Recall that if $f: A \to A$ (A finite set)
f bij $\Leftrightarrow$ f surj $\Leftrightarrow$ f inj.
φ_a is an auto iff φ_a is surj iff ~~x~~ the powers of x^a exhaust the whole of C_n iff $\mathrm{ord}(x^a)=n$ iff a coprime to n. $\square$.

$\mathrm{Aut}(C_8)=\{\varphi_1,\varphi_3,\varphi_5,\varphi_7\}$ a coprime to 8.
$\mathrm{Aut}(C_8)$ has 4 elements. Try it and see which group you get.

$\mathrm{Aut}(C_9)=\{\varphi_1,\varphi_2\ \varphi_4\ \varphi_5\ \varphi_7\ \varphi_8\}$ which group?

Algebra (PC) 20th Jan 2012

(eg) $Aut(C_{12})$:

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

$Aut(C_{12}) = \{\varphi_1, \varphi_5, \varphi_7, \varphi_{11}\}$ because

1, 5, 7, 11 are the only coprimes of 12 (residues Mod 12) which are coprime to 12

OK as a set, but we need the group structure

	$\varphi_1 = 1$	φ_5	φ_7	φ_{11}
$\varphi_1 = 1$	φ_1	φ_5	φ_7	φ_{11}
φ_5	φ_5	1	φ_{11}	φ_7
φ_7	φ_7	φ_{11}	1	φ_5
φ_{11}	φ_{11}	φ_7	φ_5	1

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

$\varphi_5^2(x) = x \Rightarrow \varphi_5^2 = Id.$

$\varphi_5\varphi_7(x) = \cancel{(x^7)^5} = \varphi_5(x)^7 = (x^5)^7 = x^{35} = x^{11}$

$\varphi_5\varphi_{11}(x) = x^{55} = x^7$

$\varphi_7\varphi_5 = (x^7)^5 = x^{35} = x^{11}$

$\varphi_7\varphi_7 = x^{49} = x = Id$

Notice it's abelian because it can reflect in diagonal.
group of order 4.

$|Aut(C_{12})| = 4$. Which group have we got? C_4 or $C_2 \times C_2$?

It's $C_2 \times C_2$. $Aut(C_{12}) \cong C_2 \times C_2$. Why?

$C_2 \times C_2$ $C_2 = \langle 1, x \mid x^2 = 1 \rangle$ also... $C_2 = \langle 1, y \mid y^2 = 1 \rangle$

$(x^a, y^b)(x^c, y^d) = (x^{a+c}, y^{b+d})$

	(1,1)	(x,1)	(1,y)	(x,y)
(1,1)	(1,1)	(x,1)	(1,y)	(x,y)
(x,1)	(x,1)	(1,1)	(x,y)	(1,y)
(1,y)	(1,y)	(x,y)	(1,1)	(x,1)
(x,y)	(x,y)	(1,y)	(x,1)	(1,1)

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

$(1,1) \rightarrow 1 = \varphi_1$
$(x,1) \rightarrow \varphi_5$
$(1,y) \rightarrow \varphi_7$
$(x,y) \rightarrow \varphi_{11}$

is a group iso

How to avoid so many brackets in $G \times H$.

$C_2 \times C_2 = \{(x^a, y^b) \ldots$

Replace $(x,1)$ by X
and $(1,y)$ by Y

Can describe $C_2 \times C_2$ as $\{1, X, Y, XY \mid X^2 = 1, Y^2 = 1, YX = XY\}$

So to describe $Aut(C_{12})$ simply put $X = \varphi_5$, $Y = \varphi_7$, $\varphi_{11} = XY$
and I do have $X^2 = 1 = Y^2$ $YX = XY$ $Aut(C_{12}) \cong C_2 \times C_2$

ⓔⓖ $Aut(C_{20})$ $C_{20} = \{1, z, \dots z^{19} \mid z^{20} = 1\}$

As a set, $Aut(C_{20}) = \{\varphi_a : a \text{ coprime to } 20\}$

$\{\underset{1}{\underset{\shortparallel}{\varphi_1}}, \varphi_3, [illegible], \varphi_7, \varphi_9, \varphi_{11}, \varphi_{13}, \varphi_{17}, \varphi_{19}\}$ group of order 8

We know C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8, Q_8 which one is $Aut(C_{20})$

$\varphi_3^2 = \varphi_9$ $\varphi_3^3 = \varphi_7$ $\varphi_3^4 = Id = \varphi_1$ $\Rightarrow$ not $C_2 \times C_2 \times C_2$ because every element in that satisfies $x^2 = 1$.

$\varphi_{11}^2 = \varphi_1 = Id$ Put $X = \varphi_3$ $Y = \varphi_{11}$
$X^4 = 1$ $Y^2 = 1$

$XY = \varphi_3 \varphi_{11} = \varphi_{33} = \varphi_{13}$
$X^2Y = \varphi_9 \varphi_{11} = \varphi_{99} = \varphi_{19}$

$X^3Y = \varphi_7 \varphi_{11} = \varphi_{77} = \varphi_{17}$
Also $YX = \varphi_{11}\varphi_3 = \varphi_{13} = XY$

$$\left\{\begin{array}{cccccccc} 1 & X & X^3 & X^2, & Y, & XY, & X^3Y, & X^2Y \\ \varphi_1 & \varphi_3 & \varphi_7 & \varphi_9 & \varphi_{11} & \varphi_{13} & \varphi_{17} & \varphi_{19} \end{array}\right\}$$

$|Aut(C_{20})| = 8$

$Aut(C_{20}) = \{1, X, X^3, X^2, Y, XY, X^2Y, X^3Y \mid X^4 = 1, Y^2 = 1, YX = XY\}$
$\cong C_4 \times C_2$
$\langle X \rangle \langle Y \rangle$

Prop: The automorphism group of a cyclic group is always abelian. ie $Aut(C_n)$
Not true for non-cyclic groups

Pf: $Aut(C_n) = \{\varphi_a : (a,n) = 1\}$ $n = \{1, x, \dots, x^{n-1}\}$

$$\varphi_a\varphi_b(x) = \varphi_a(x^b) = \varphi_a(x)^b = (x^a)^b = \underbrace{x^{ab} = x^{ba}}_{\text{multiplication is commutative}} = (x^b)^a = \varphi_b(x^a) = \varphi_b\varphi_a(x)$$

$\Rightarrow \varphi_a\varphi_b(x) = \varphi_b\varphi_a(x)$

Algebra 20th Jan 2012

Subgroups:

Let $G = (G, \cdot, 1)$ be a group

Let $H \subset G$ be a subset

What conditions must H satisfy to be a group itself?

Need i) $1 \in H$

ii) $\forall x, y \in H \quad xy \in H$ - Closure (prop of subgroups, NOT groups)

iii) if $x \in H$ then $x^{-1} \in H$

Defn: Let $H \subset G$. G group. Say that H is a subgroup of G when

i) $1 \in H$

ii) $\forall x, y \in H \quad xy \in H$

iii) $\forall x \in H \quad x^{-1} \in H$.

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

Is $\{1, x\}$ a subgroup?

no, $x^2 \notin \{1, x\}$

$x^{-1} = x^2$ doesn't belong to $\{1, x\}$

Is $\{1, x, x^2\}$ a subgroup? Yes.

Is $\{1, y\}$ a subgroup? Yes.

Is $\{1, x, y, xy\}$ a subgroup? No.

In fact the subgroups of D_6 are as follows.

D_6, $\{1\}$ obvious ones.

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

Orders: 6, 1, 3, 2, 2, 2

Thm - Lagranges Thm (Done before but going over again)

Let G be a finite group, and $H \subset G$ a subgroup, then $\underset{\text{order of } H}{|H|}$ divides $|G|$ exactly

In order to prove the thm we need the notion of a COSET

Defn: Let H be a subgroup of G and let $z \in G$

Define $zH = \{zh : h \in H\}$ zH is called the left coset of H by z

Define $Hz = \{hz : h \in H\}$ Hz is called the right coset...

Normally use left coset

(eg) $G = D_6 \longrightarrow$

Take $H = \{1, y\}$, subgroup.

List the cosets:

$1H = \{1\cdot 1, 1\cdot y\} = \{1, y\} = H$

$xH = \{x\cdot 1, x\cdot y\} = \{x, xy\}$

$x^2H = \{x^2, x^2y\}$

$yH = \{y, 1\} = \{1, y\} = H$

$xyH = \{xy, x\} = \{x, xy\}$

$x^2yH = \{x^2y, x^2\} = \{x^2, x^2y\}$

So we have 3 distinct left cosets, each listed twice : $\{1,y\}, \{x,xy\}, \{x^2,x^2y\}$

Defn: H subgroup of G.

$$\boxed{\begin{aligned} G/H &= \{gH : g \in G\} \\ H\backslash G &= \{Hg : g \in G\} \end{aligned}}$$

set of left cosets. read G/H : G mod H.

set of ~~left~~ right cosets.

So... $H = \{1, y\} \subset D_6 = G$ then

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

(eg) $K = \{1, x, x^2\} \subset D_6$

$1K = xK = x^2K = \{1, x, x^2\}$

$yK = xy\cdot K = x^2yK = \{y, xy, x^2y\}$ ‖ check!

Basic Properties of Cosets (left)

Let H be a subgroup of G

Consider wH, zH , $(w, z \in G)$

i) Either $wH = zH$ OR $wH \cap zH = \emptyset$

(ie either theyre the same or completely different)

Pf of i) Enough to prove that if $wH \cap zH \neq \emptyset$ then $wH \equiv zH$.

So suppose $\exists\, k \in wH \cap zH$

so $\exists\, h_1 \in H$ $k = wh_1$ and $\exists\, h_2 \in H$ $k = zh_2$

so $w = zh_2h_1^{-1}$

Let $\eta \in wH$. $\eta = wh_3$, some $h_3 \in H$

$\eta = wh_3 = z(h_2h_1^{-1}h_3)$ and $h_2h_1^{-1}h_3 \in H$ so

$\eta \in zH$ ie $wH \subset zH$

By symmetry $zH \subset wH$

So I've shown that if $wH \cap zH \neq \emptyset$ then

$wH \subset zH \subset wH$ ie $wH \equiv zH$ $\boxed{i}$

ii) Rule of equality for cosets.

When is $g_1H = g_2H$?

Ans: $g_1H = g_2H \iff g_1^{-1}g_2 \in H$

Proof ($\Rightarrow$) Suppose $g_1H = g_2H$

$g_2 \in g_2H$ $\quad g_2 = g_2 \cdot 1$

So $g_2 \in g_1H$ so $g_2 = g_1h$ for some $h \in H$.

so $g_1^{-1}g_2 = h \in H$ $\boxed{\Rightarrow}$

($\Leftarrow$) Suppose $g_1^{-1}g_2 \in H$ $\quad g_1^{-1}g_2 = h\ (\in H)$

so $g_1g_1^{-1}g_2 = g_1h$ $\quad g_2 = g_1h \in g_1H$

but $g_2 \in g_2H$ $\quad (g_2 = g_2 \cdot 1)$

So $g_1H \cap g_2H \neq \emptyset$ so $g_1H = g_2H$ by (i) above. $\boxed{\Leftarrow}$

iii) There is a bijective mapping

$H \longrightarrow gH$ (for any $g \in G$)

Proof: $\lambda_g : H \to gH$ $\quad \lambda_g(h) = gh$

λ_g is obviously surjective (by defn of gH)

λ_g is injective $\lambda_g(h_1) = \lambda_g(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow g^{-1}gh_1 = g^{-1}gh_2$

$\Rightarrow h_1 = h_2$ $\boxed{iii}$.

In numerical terms, (iii) is (iii)'. If H is finite then $|gH| = |H|$ $\forall g \in G$

Corallary (Lagrange)

Let G be a finite group, $H \subset G$ a subgroup. Then $|H|$ divides $|G|$ exactly

Proof: Write out the distinct cosets of H: $g_1H, g_2H, \dots, g_kH$ making sure that you don't write the same coset twice.

$\forall g \in G$ $\exists i$; $g \in g_iH$ (otherwise you've missed a coset)

$$G = \bigcup_{i=1}^{k} g_i H \quad . \quad g_i H \cap g_j H = \emptyset \quad i \neq j$$

So no double counting.

$$|G| = |g_1 H| + |g_2 H| + \dots + |g_k H|$$

$$= |H| + |H| + \dots + |H| \quad k \text{ times.}$$

$$|G| = k|H| \quad \square.$$

Notice in the above, $k = |G/H|$ = no. of distinct cosets.

So get

<u>Corollary</u>: $|G| = |G/H| |H|$

<u>or</u> $\frac{|G|}{|H|} = |G/H|$

Algebra 24th Jan 2012

Lagranges Thm:

Let G be a finite group and $H < G$ a subgroup. Then

i) $|H|$ divides $|G|$ exactly

ii) $|G|/|H| = |G/H|$ → no. of distinct (left) of H in G

Corollary: Let p be a prime and let G be a group. $|G| = p$

Then $G \cong C_p$

Pf: Let $x \in G$ $x \neq 1$. Let $H = \{x^a : a \in \mathbb{Z}\}$

H is a subgroup of G, $H \neq \{1\}$ $x \neq 1$

$|G| = p$, prime and $|H|$ divides $|G|$. Then $|H| = 1$ or $|H| = p$. But $|H| \neq 1$ so $|H| = p$.

So $H = \{1, x, \dots, x^{p-1}\} \cong C_p$ $\square$.

n	$G : \lvert G\rvert = n$	complete?
1	$\{1\}$	✓
2	C_2	✓
3	C_3	✓
4	C_4, $C_2 \times C_2$	?
5	C_5	✓
6	C_6, D_6	?
7	C_7	✓
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} $(\cong C_5 \times C_2)$, D_{10}	
11	C_{11}	✓
12	C_{12}, $C_6 \times C_2$, D_{12}, $\textcircled{A_4}$, $D_6^* \cong Q_{12}$	?
13	C_{13}	✓
14	C_{14}, D_{14}	?

prime have only one group.

Prop $C_m \times C_n$ m, n coprime.

Then $\cong C_{mn}$

Pf $\langle X, Y \quad X^m = 1, Y^n = 1, YX = XY \rangle$

Check that $\mathrm{ord}(XY) = mn$.

Kernels and Images

Let $h: G \to H$ be a group homomorphism.

Define $Ker(h) = \{x \in G : h(x) = 1\}$ ← Using multiplicative notation.

$Im(h) = \{y \in H : \exists x \in G : h(x) = y\}$

Prop: With the above notation, i) $Ker(h)$ is a subgroup of G,
ii) $Im(h)$ is a subgroup of H.

Pf: i) $1 \in Ker(h)$ as $h(1) = 1$

If $x_1, x_2 \in Ker(h)$ $h(x_1) = 1$, $h(x_2) = 1$ then

$h(x_1, x_2) = h(x_1)h(x_2) = 1 \cdot 1 = 1$. So $x_1 x_2 \in Ker(h)$

$\Rightarrow x_1 x_2 \in Ker(h)$ [closed]

If $x \in Ker(h)$ $h(x) = 1$

$h(x^{-1}) = h(x)^{-1} = 1^{-1} = 1$ so $x^{-1} \in Ker(h)$ $\boxed{i}$

ii) $1 \in Im(h)$ because $h(1) = 1$

If $y_1, y_2 \in Im(h)$ then write $h(x_1) = y_1$, $h(x_2) = y_2$ for some $x_1, x_2 \in G$. Then $h(x_1, x_2) = h(x_1)h(x_2) = y_1 y_2$ so $y_1 y_2 \in Im(h)$ [closed].

Finally, $y \in Im(h)$. Write $y = h(x)$ then

$h(x^{-1}) = h(x)^{-1} = y^{-1}$ so $y^{-1} \in Im(h)$ $\boxed{ii} \Rightarrow \boxed{}$.

$h: G \to H$.

By Lagrange's Thm: $|Im(h)|$ divides $|H|$. Also, $|Ker(h)|$ divides $|G|$

We'll show that $|Im(h)|$ also divides $|G|$

We'll show:

Thm: Let $h: G \to H$ be a group homo. Then $\exists$ a bijection:

$$\boxed{G/Ker(h) \longrightarrow Im(h)}$$

In particular, $|Im(h)| = \frac{|G|}{Ker(\varphi)}$

or $|Im(h)||Ker(\varphi)| = |G|$ equivalent of Kernel-Rank Thm.

Pf: Put $K = Ker(h)$ so K is a subgroup of G.

The elements of G/K (G mod K) are sets of the form:

$xK = \{xk : k \in K\}$ where $x \in G$.

Recall...

Rule of Equality

$x_1 K = x_2 K \iff x_2^{-1} x_1 \in K$

Define a mapping $h_* : G/K \longrightarrow \mathrm{Im}(h)$ as follows.

$h_*(xK) = h(x)$. To complete the proof, need to show

a) h_* is well defined

b) $h_* : G/K \longrightarrow \mathrm{Im}(h)$ injective

c) $h_* : G/K \longrightarrow \mathrm{Im}(h)$ surj.

Proof: a) Suppose $x_1 K = x_2 K$. Need to show that $h(x_1) = h(x_2)$. If $x_1 k = x_2 k$ from Rule of Eq., we know $x_2^{-1} x_1 \in K = \ker(h)$. So apply h to $x_2^{-1} x_1$.

$h(x_2^{-1} x_1) = 1$ because it belongs in $\ker(h)$.

So $h(x_2^{-1}) h(x_1) = 1$ so $h(x_2)^{-1} h(x_1) = 1$

So $h(x_1) = h(x_2)$ $\boxed{a}$.

b) Suppose $h_*(x_1 K) = h_*(x_2 K)$ then $h(x_1) = h(x_2)$ so $h(x_2)^{-1} h(x_1) = 1$ so $h(x_2^{-1} x_1) = 1$ so $x_2^{-1} x_1 \in K$

$\Rightarrow x_1 k = x_2 k$. $\boxed{b}$

c) Is obvious.

If $y \in \mathrm{Im}(h)$ write $y = h(x)$ so $h_*(xk) = y$ $\boxed{c} \Rightarrow \boxed{}$.

Corollary: if $h : G \longrightarrow H$ is a group homo, then $|\mathrm{Im}(h)|$ divides both $|G|$ and $|H|$.

We'll apply this as follows. Suppose $n \geq 1$ and Γ some finite group. Want to be able to write down all homomorphisms $h : C_n \longrightarrow \Gamma$

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

$\mathrm{Im}(h) = \{1, h(y), \dots, h(y)^{n-1}\}$ possibly with repetitions.

Need $\mathrm{ord}(h(y))$ to divide both $|\Gamma|$ (ok by Lagrange) and also n (by last result)

$C_4 = \{1, y, y^2, y^3 \mid y^4=1\} \xrightarrow{h} C_6\{1, \ldots, x^5 \mid x^6 = 1\}$

i) $h(1) = 1$

$\boxed{h(y) = x\ ?}$ no.

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

$h(y^3) = x^3$

$h(y^4) = x^4$

so $h(1) = x^4 \neq 1$

ii) $h(1) = 1$

$\boxed{h(y) = x^4 ?}$ no

$h(y^2) = x^8 = x^2$

$h(y^3) = x^{12} = 1$

$h(y^4) = x^4$

~~$h(y^5) = x^2$~~ $y^4 = 1$ and $x^4 \neq 1$ so)

~~$h(y^6) =$~~

iii) $h(1) = 1$

$\boxed{h(y) = x^3 ?}$ YES

$h(y^2) = 1$

$h(y^3) = x^3$

$h(y^4) = 1$ ☺

$h(y^m) = x^{3m}$ gives a homo.

i) ord $y = 4$
ord $x = 6$

6 doesn't divide 4.

ii) ord $x^4 = 3$, 3 doesn't divide 4.

Thm: Let Γ be a finite group, $\gamma \in \Gamma$. Then $\exists$ homomorphism $h : C_n \to \Gamma$ st $h(y) = \gamma$ iff ord(γ) divides n.

$C_n = \{1, y, \ldots, y^{n-1}\}$

Pf: Write ord$(\gamma) = m$. $\langle \gamma \rangle = \{1, \ldots, \gamma^{m-1}\}$ is a subgp of order m.
Suppose $\exists$ homo $h : C_n \longrightarrow \Gamma$ st $h(y) = \gamma$.
Then $\mathrm{Im}(h) = \langle \gamma \rangle$ and we know $|\mathrm{Im}(h)|$ divides n.
(Last thm) So if $\exists h : C_n \to \Gamma$ such that $h(y) = \gamma$ then ord(γ) must divide n. Conversely, if $\gamma \in \Gamma$ is such that ord(γ) divides n then define

$$h_\gamma : C_n \to \Gamma \text{ by } h_\gamma(y^r) = \gamma^r$$

Then h_r is a homo.

$$\left.\begin{aligned} h_r(y^a) &= \gamma^a \\ h_r(y^b) &= \gamma^b \end{aligned}\right\} \quad h_\gamma(y^{a+b}) = \gamma^{a+b} = \gamma^a \gamma^b = h_\gamma(y^a) h_\gamma(y^b) \quad \square.$$

~~Again~~ Again, homo's

$$\{1, y, y^2, y^3\} = C_4 \xrightarrow{h} C_6 \quad \{1, x, \dots x^5\}$$

What are the possible values of $h(y)$? Can I send:

$y \to 1$? Yes 1 divides 4

$y \to x$? No $6 \nmid 4$

$y \to x^2$? No $3 \nmid 4$

$y \to x^3$? Yes $2 \mid 4$

x^4? No $3 \nmid 4$

x^5? No $6 \nmid 4$

Orders	1	6	3	2	3	6
	$\{1$	x	x^2	x^3	x^4	$x^5\}$

So

ⓔⓖ There are precisely two homos $h : C_4 \to C_6$

1) $h(y) = 1$ so $h(y^r) = 1$ for all r trivial homo.

2) $h(y) = x^3$ $\quad h(y^r) = x^{3r}$

ⓔⓖ Describe all homos. $C_9 \to C_2 \times C_6$

$C_9 = \{1, y, \dots y^8 \mid y^9 = 1\}$ $\quad C_2 \times C_6 = \{X^{\overset{a}{\bullet}} Z^{\overset{b}{\bullet}} \mid X^2 = 1 \;\; Z^6 = 1 \;\; ZX = XZ\}$?

$C_2 \times C_6 = \{1, X, Z, XZ, Z^2, XZ^2, Z^3, XZ^3, Z^4, XZ^4, Z^5, XZ^5\}$

	✓				✓				✓			
orders:	1	2	6	6	3	6	2	2	3	6	6	6
	$1 \nmid 9$	$2 \nmid 9$	$6 \nmid 9$	$6 \nmid 9$	$3/9$							

$y \to 1$ Trivial homo $h(y^r) = 1 \;\; \forall r$

$y \to z^2$ $h(y^r) = z^{2r}$ $\quad 3 \mid 9.$

$y \to z^4$ $h(y^r) = z^{4r}$ $\quad 3 \mid 9.$

So there are exactly three homos $C_9 \to C_2 \times C_6$

Want to construct <u>new groups</u> by generalising the structure of D_6 .. (D_{2n})

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

Subgroups: $C_3 = \{1, x, x^2\}$ $\quad C_2 \{1, y\}$

$yx = x^2y$ $\quad$ $yxy^{-1} = x^2$

Operator homomorphism:

Suppose G is a group. $Q \subset G$ is a subgroup.

Consider $z \to qzq^{-1}$, $q \in Q$??

Define $\left[\begin{array}{l} c: Q \longrightarrow \mathrm{Aut}(G) \\ c(q)(z) = qzq^{-1} \end{array}\right.$

Prop: Let G be a group, $q \in G$. Then the mapping

$\left.\begin{array}{l} G \longrightarrow G \\ z \longmapsto qzq^{-1} \end{array}\right\}$ is an automorphism of G.

$C_q(z) = qzq^{-1}$, $\quad C_q \in \mathrm{Aut}(G)$

Proof: • C_q is a homo. $\qquad$ Insert cancelling power $q^{-1}q = 1$.

$C_q(z_1z_2) = q(z_1z_2)q^{-1} = (qz_1q^{-1})(qz_2q^{-1}) = C_q(z_1)C_q(z_2)$

and C_q is a homo as claimed.

• C_q is injective $\quad C_q(z_1) = C_q(z_2)$

$qz_1q^{-1} = qz_2q^{-1}$: left mutiply by q^{-1}, right by q

$q^{-1}qz_1q^{-1}q = q^{-1}qz_2q^{-1}q \Rightarrow z_1 = z_2$

$C_q(z_1) = C_q(z_2) \Rightarrow z_1 = z_2$.

• C_q is surj:

If $z \in G$ write $w = q^{-1}zq$

$C_q(w) = qq^{-1}zqq^{-1} = z$ so $C_q: G \to G$ is an automorphis $\square$.

Prop: Let G be a group, Q subgroup. $Q \subset G$.

Consider the mapping $c: Q \to \mathrm{Aut}(G)$, $q \longmapsto C_q$.

$(c(q) = C_q)$ Then c is a homo.

Proof: Let $q_1, q_2 \in Q$. Need to show $C_{q_1q_2} = C_{q_1} \circ C_{q_2}$ $\qquad$ composition.

$C_{q_1q_2}(z) = (q_1q_2)(z)(q_1q_2)^{-1}$ But $(q_1q_2)^{-1} = q_2^{-1}q_1^{-1}$

So $C_{q_1q_2}(z) = q_1(q_2zq_2^{-1})q_1^{-1} = C_{q_1}(q_2zq_2^{-1}) = C_{q_1}(C_{q_2}(z))$

$= (C_{q_1} \circ C_{q_2})(z)$ $\square$.

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

$Q = \{1, y\} = C_2$

Get $c : C_2 \longrightarrow \mathrm{Aut}(G)$

$c_y(g) = ygy^{-1}$ homomorphism

<u>Defn</u>: A subgroup K of G is said to be normal in G $(K \triangleleft G)$ when for each $g \in G$ each $k \in K$

$gkg^{-1} \in K$ $\{1, x, x^2\} \triangleleft D_6$.

Actually got $c : C_2 \longrightarrow \mathrm{Aut}(C_3)$ $y \longmapsto \tau$. $\tau(x) = x$

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

Algebra (PC) 27th Jan 2012

2)ii) $\varphi : G \to H$ *injective* homo

if $x^n = 1$ $\quad \varphi(x^n) = \varphi(x)^n$

$\varphi(1) = 1 \Rightarrow \varphi(x)^n = 1$

$\text{ord}\, \varphi(x) \le \text{ord}(x)$ because INJECTIVE

Suppose $1 \le \text{ord}\, \varphi(x) < n$)

then $\exists r, 1 \le r < n$ $\quad \varphi(x)^r = 1 \quad \varphi(x^r) = 1^{(*)}$

But also $\varphi(1) = 1^{(**)}$

(*) and (**) φ injective so $x^r = 1$ and $r < n$ contradicts defn of order(x

vi) $C_3 \times C_4 \cong C_{12}$? Yes but why

Got to produce an explicit isomorphism

$C_3 = \{1, x, x^2\}$ $\quad C_4 = \{1, y, y^2, y^3\}$ $\quad C_{12} = \{1, z, \dots z^{11}\}$

$C_{12} \longrightarrow C_3 \times C_4$

Define

$\varphi(1) = (1,1)$ $\qquad \varphi(z^6) = (1, y^2)$

$\varphi(z) = (x, y)$ $\qquad \varphi(z^7) = (x, y^3)$

$\varphi(z^2) = (x^2, y^2)$ $\qquad \varphi(z^8) = (x^2, 1)$

$\varphi(z^3) = (1, y^3)$ $\qquad \varphi(z^9) = (1, y)$

$\varphi(z^4) = (x, 1)$ $\qquad \varphi(z^{10}) = (x, y^2)$

$\varphi(z^5) = (x^2, y)$ $\qquad \varphi(z^{11}) = (x^2, y^3)$

$\varphi(z^a) = (x,y)^a$

$\varphi(z^a z^b) = \varphi(z^{a+b}) = (x,y)^{a+b} = (x,y)^a (x,y)^b = \varphi(z^a)\varphi(z^b)$

so φ is a homo and bijective

Many people observed that if $G = C_{12}$ $\quad H = C_3 \times C_4$

then $|G(n)| = |H(n)|$ $\forall n$.

In general it is false that if $|G(n)| = |H(n)|$ $\forall n$ then $G \cong H$.

Algebra 27th Jan 2012

I'll show that if p is an odd prime and $|G| = 2p$ then either $G \cong C_{2p}$ or $G \cong D_{2p}$

Prop: let G be a group in which each element g satisfies $g^2 = 1$. Then G is abelian.

Pf: let $x, y \in G$. I have to show $yx = xy$. I know that $x^2 = 1$, so $x^{-1} = x$. Also $y^2 = 1$ so $y^{-1} = y$. Also $(xy)^2 = 1$ so $(xy)^{-1} = xy$. But $(xy)^{-1} = y^{-1}x^{-1}$ and in this case $y^{-1} = y$, $x^{-1} = x$ so $(xy)^{-1} = yx$. But $(xy)^{-1} = xy = yx$ □.

We can improve on this:

Better Result: let G be a finite group in which $\forall g \in G$, $g^2 = 1$

Then i) $G \cong \underbrace{C_2 \times C_2 \times \dots \times C_2}_{n}$ for some n.

so ii) $|G| = 2^n$

Pf: Know that G is abelian so I will temporarily use additive notation.

$g^2 = 1 \Rightarrow g + g = 0 \ (= 2g)$

So regard G as a vector space over field $\mathbb{F}_2 = \{0,1\}$

Apply Basis Thm. Then as a vector space:

$$G \cong \underbrace{\mathbb{F}_2 \oplus \dots \oplus \mathbb{F}_2}_{n} \qquad n = \dim_{\mathbb{F}_2} G$$

As groups $G \cong \underbrace{\mathbb{F}_2 \times \dots \times \mathbb{F}_2}_{n}$ so $|G| = |\underbrace{\mathbb{F}_2 \times \dots \times \mathbb{F}_2}_{n}| = 2^n$

$\underset{\text{additive}}{\mathbb{F}_2} \cong \underset{\text{mult.}}{C_2}$ So $G \cong \underbrace{C_2 \times \dots \times C_2}_{n}$ □.

$\{0,1\} = \{1, x\}$

$0 \longrightarrow 1$

$1 \longrightarrow x$

Now let G be a finite group $|G| = 2p$ where p is odd prime.

claim (I) G has an element of order p

and (II) G has an element of order 2.

Proof I : If $z \in G$ known (by Lagrange)

either $\mathrm{ord}(z)=1$ $\underbrace{\mathrm{ord}\, z = 2 \quad \mathrm{ord}\, z = p \quad \mathrm{ord}\, z = 2p}_{\text{non trivial}}$,

$z=1$

If $z \neq 1$ then $\nearrow$

It cannot be true that every $z \in G$ $z \neq 1$ has $\mathrm{ord}\, z = 2$

Otherwise $|G| = 2^n$ (by last result) So suppose $z \in G$, $z \neq 1$, $\mathrm{ord}\, z \neq 2$. Either $\mathrm{ord}\, z = p$ and we're proved I or $\mathrm{ord}\, z = 2p$, then $\mathrm{ord}\, z^2 = p$. Either way, I is true $\square$.

$\downarrow$

$(z^{2p} = 1 \ , (z^2)^p = 1)$.

Proof II : Let $z \in G$, $\mathrm{ord} z = p$.

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

$|G/k| = 2$, $G = k \sqcup gk$ for some $g \in G$, $g \notin k$

($\sqcup$: disjoint union : $G = k \cup gk$ $k \cap gk = \emptyset$)

Suppose $\gamma \in gk$. Then $\overset{\text{claim}}{}$ $\gamma^2 \in k$ $(\gamma k \neq k)$

Otherwise $\gamma^2 \in gk$ $\gamma^2 k = \gamma k$

and $\gamma^{-1}\gamma^2 k = \gamma^{-1}\gamma k$

$\gamma k = k$ ✗.

So if $\gamma \notin k$ then $\gamma^2 \in k$, what are possibilities for γ^2?

: $\{1, z, z^2, \dots, z^{p-1}\}$

if $\gamma^2 = 1$ then $\mathrm{ord}(\gamma) = 2$. Finished

If $\gamma^2 = z^a$ $1 \leq a \leq p-1$ $\mathrm{ord}(\gamma^2) = p$

so $\mathrm{ord}(\gamma) = 2p$ so $\mathrm{ord}(\gamma^p) = 2$

either way I have an element of order 2 $\square$.

So we're trying to prove that if $|G| = 2p$ then

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

Shown G has an element x $\mathrm{ord}(x) = p$

" " " y $\mathrm{ord}(y) = 2$

Take $K = \{1, x, \dots, x^{p-1}\}$ $G = K \sqcup yK$ $y \notin K$

also $G = K \sqcup Ky$ so $\boxed{yK = Ky}$

Get a map $h_y : K \longrightarrow K$ $h_y = h$ sub k.

$x^a \longmapsto y x^a y^{-1}$

$h_y(k) = yky^{-1}$

h_y is an automorphism of K

$h_y(k_1k_2) = y(k_1k_2)y^{-1} = (yk_1y^{-1})(yk_2y^{-1}) = h_y(k_1)h_y(k_2)$

homomorphism

$h_y^2 = Id$ so BIJECTIVE.

So $h_y \in Aut(K) \cong Aut(C_p)$ and $h_y^2 = Id$

Prop: let $\alpha : C_p \to C_p$ be an automorphism s.t $\alpha^2 = Id$

Then either $\alpha = Id$ or $\alpha(x) = x^{-1}$.

Proof: let $x \in C_p$ be generator.

Put $z = \alpha(x)x \in C_p$. Then $ord(z) = 1$ or $ord(z) = p$.

$ord(z) = 1$ means $z = 1$ ie $\alpha(x) = x^{-1}$

If $ord(z) = p$ then z generates C_p, and $\alpha(z) = \alpha(\alpha(x)x)$

$= \alpha^2(x)\alpha(x)$, $\alpha^2 = 1$, $= x\alpha(x)$

But C_p albelian so $x\alpha(x) = \alpha(x)x = z$ SO

$\alpha(z) = z$ Hence $\alpha = Id$ $\square$.

Thm: let p be an odd prime $|G| = 2p$ ..

Then either $G \cong D_{2p}$ or $G \cong C_{2p}$.

Pf: let $x \in G$ have $order(x) = p$

$y \in G$ . . . $ord(y) = 2$

Consider $\alpha = h_y : K \longrightarrow K$ $K = \{1, x, \dots x^{p-1}\}$

$\alpha^2 = 1$ so either

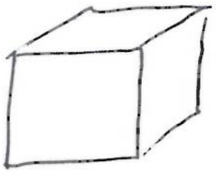
$\alpha(x) = x^{-1}$ or $\alpha(x) = x$

$\alpha = h_y$ $\alpha(x) = yxy^{-1}$ so either

$yxy^{-1} = x^{-1}$ or $yxy^{-1} = x$

$yxy^{-1} = x^{p-1}$ $\Downarrow$ $yx = xy$

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



n	G	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	✓
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, Q_8, D_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}	?

Algebra 31st Jan 2012

To show $|G| = 2p \Rightarrow G \cong D_{2p}$ and $G \cong C_{2p}$

We constructed within G two subgroups $K = \{1, x, \dots, x^{p-1} \mid x^p = 1\}$

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

The point at issue was

Defn $yx = ? = x^a y$

Semidirect product

$$\boxed{K \rtimes_h Q}$$

Data: (i) Groups K, Q

(ii) a homomorphism $h : Q \to \mathrm{Aut}(K)$

auto acting on k_2

Try to define a multiplication on $K \times Q$ (cross)

$h(q_1)(k_2)$

$\boxed{K \rtimes_h Q}$ $* : (K \times Q) \times (K \times Q) \to (K \times Q)$

mK mQ

$$\boxed{(k_1, q_1) * (k_2, q_2) = (k_1 \cdot h(q_1)(k_2), q_1 \cdot q_2)}$$

Standard mult

$h(q_1) \in \mathrm{Aut}(K)$ so $h(q_1)$ acts on $k_2 \in K$ to give $h(q_1)(k_2) \in K$

Set as a hmwk that $*$ is a group mult on the set $K \times Q$

Prop: $(1,1)$ is the identity for $K \rtimes_h Q$

Pf: $(1,1) * (k,q) = (1 \cdot h(1)(k), 1 \cdot q) = (k, q)$

$h : Q \to \mathrm{Aut}(K)$ is a homo so $h(1) = \mathrm{Id}$. so $h(1)(k) = k$

so $(1,1)$ is left Identity

$(k,q) * (1,1) = (k \cdot h(q)(1), q \cdot 1)$ But $h(q) \in \mathrm{Aut}(K)$ so $h(q)(1) = 1$

$= (k \cdot 1, q \cdot 1) = (k, q) \Rightarrow (1,1)$ is the right Identity.

$k, k_1, k_2 \in K$ $q, q_1, q_2 \in Q$

There are 4 special products

(I) $(k_1, 1) * (k_2, 1)$

(II) $(k, 1) * (1, q)$

(III) $(1, q) * (k, 1)$ ← !!

(IV) $(1, q_1) * (1, q_2)$

(I), (II) and (IV) cause no surprise.

(I) $(k_1,1)*(k_2,1) = (k_1k_2\ ,1)$

Pf: $(k_1,1)*(k_2,1) = (k_1h(1)(k_2)\ ,1\cdot 1) = (k_1k_2,1)$

$h(1) = \mathrm{Id} \in \mathrm{Aut}(K)$ so $h(1)(k_2) = k_2$

(II) $(k,1)*(1,q) = (k,q)$

Pf: $(k,1)*(1,q) = (k\,h(1)(1)\ ,\ 1\cdot q) = (k,q)$

(IV) $(1,q_1)*(1,q_2) = (1,q_1q_2)$

Pf: $(1\cdot h(q_1)(1)\ ,\ q_1\cdot q_2)$

$h(q_1)$ is an ~~homo~~ auto of K so $h(q_1)(1)=1$.

$= (1,q_1q_2)$ □.

(eg) of a "crucial calculation" like III

$K = C_3 = \{1,x,x^2\}$ $\quad Q = C_2 = \{1,y\}$

I know $\mathrm{Aut}(K) = \mathrm{Aut}(C_3) \cong C_2 = \{1,\tau\}$ where $\tau(x) = x^2$

Let $h : C_2 \longrightarrow \mathrm{Aut}(C_3$ $\quad$ || h is nontrivial homomorphism.

$h(1) = 1 \quad \boxed{h(y) = \tau}$

Form $\boxed{C_3 \rtimes_h C_2}$

Crucial calculation:

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

If I now write $X = (x,1)$ $\quad Y = (1,y)$

$Y*X = (x^2,y) = (x^2,1)(1,y) = X^2Y \Rightarrow YX = X^2Y \ : D_6.$

Question: What happens if I take the trivial homo

$\eta : C_2 \longrightarrow \mathrm{Aut}(C_3)$ $\quad \eta(1) = 1,\ \eta(y) = 1$

Form $C_3 \rtimes_\eta C_2$ and do crucial calc

$Y*X = (1,y)*(x,1) = (1\cdot\eta(y)(x)\ ,\ y\cdot 1)$ $\quad (\eta(y) = \mathrm{Id}. \Rightarrow \eta(y)(x) = x)$

$= (x,y) = (x,1)*(1,y) = XY.$ $\quad X^3 = 1 \quad Y^2 = 1$

With the trivial homo we get the direct product $C_3 \times C_2$

→ Always the case

Prop: If $h : Q \to \mathrm{Aut}(K)$ is a trivial homo then $K \rtimes_h Q = K \times Q$

Direct product.

Pf: Do the crucial calc.

$$(1,q)*(k,1) = (1 \cdot h(q)(k), q \cdot 1) = (k,q) = (k,1)*(1,q) \quad \square$$

Because $h(q) = \mathrm{Id}$ (Trivial)

So now we can construct some new groups......

Nonabelian group of order 21

$21 = 7 \times 3$ Take $K = C_7$, $Q = C_3$

Now we need homos $h : C_3 \to \mathrm{Aut}(C_7) \cong C_6$

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

Put $\alpha = \varphi_3$ $\alpha^2 = \varphi_9 = \varphi_2$ (mod 7)

$\alpha^3 = \varphi_6$ $\alpha^4 = \varphi_4$ $\alpha^5 = \varphi_5$ $\alpha^6 = 1$

$\mathrm{Aut}(C_7) = \{\mathrm{Id}, \alpha_2, \alpha, \alpha^4, \alpha^5, \alpha^3\}$

Now for homos $C_3 \to C_6$ $(= \mathrm{Aut}(C_7))$

h_1 $1 \to 1$, $y \to \alpha^2$, $y^2 \to \alpha^4$ | not α, order $6 \nmid 3$ no. so $y \to \alpha^2$

h_2: $1 \to 1$, $y \to \alpha^4$, $y^2 \to \alpha^2$ | α^3 ord $2 \nmid 3$ ord $\alpha^4 = 3$ $3 \mid 3$ so yes

non trivial

$1 \to 1$, $y \to 1$, $y^2 \to 1$ | trivial

So let's take $h_1 : C_3 \to \mathrm{Aut}(C_7)$ $\quad h_1(y) = \alpha^2$

from $C_7 \rtimes_{h_1} C_3$ and do the crucial calc

$$(1,y)*(x,1) = (1, h_1(y)(x), y\cdot 1) = (x^2, y) = (x^2,1)(1,y)$$

$$h_1(y) = \alpha^2 \qquad \alpha^2(x) = (\varphi_2(x)) = x^2 \,]$$

$$\Rightarrow YX = X^2Y$$

So we have a new group $G(21)$ with following generators X, Y and relations $X^7 = 1$, $Y^3 = 1$, $YX = X^2Y$

Question: What happens if we take

$$h_2 : C_3 \to \mathrm{Aut}(C_7)$$

We have three homos $C_3 \to \mathrm{Aut}(C_7)$

- h_0 = trivial homo

  $C_7 \rtimes_{h_0} C_3$ generators X, Y $\quad X^7 = 1,\ Y^3 = 1,\ YX = XY$

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

- $h_1 : C_3 \to \mathrm{Aut}(C_7)$ $\quad h_1(y) = \varphi_2 (= \alpha^2)$ $\quad$ nonabelian

  $C_7 \rtimes_{h_1} C_3$ $\quad X^7 = Y^3 = 1$ but now $YX = X^2Y$

- $h_2 : C_3 \to \mathrm{Aut}(C_7)$ $\quad h_2(y) = \varphi_4 (= \alpha^4)$ $\quad h_2(y)(x) = x^4$

  Crucial calc gives $YX = X^4Y$, $X^7 = Y^3 = 1$. nonabelian

APPARENTLY we get 3 semidirect products.

$C_7 \times C_3$, $\langle X, Y \mid X^7 = 1 = Y^3,\ YX = XY \rangle$ $\quad C_7 \rtimes_{h_0} C_3$

$C_7 \rtimes_{h_1} C_3$ $\langle X, Y \mid X^7 = Y^3 = 1,\ YX = X^2Y \rangle$ $\quad G(21)$

$C_7 \rtimes_{h_2} C_3$ $\langle X, Y \mid X^7 = Y^3 = 1,\ YX = X^4Y \rangle$ $\quad G(21)'$

In fact,

Prop: $G(21)' \cong G(21)$

Pf: $C_3 =$ ~~$\{1,x,x^2$~~ $\{1,y,y^2\}$ and I chose y

$= \{1,z,z^2\}$ where $z = y^2$ $(y^2)^2 = y$

For $h_1 : C_3 \to \mathrm{Aut}(C_7)$

$h_1(y) = \varphi_2$ so

$h_1(z) = \varphi_4 = \varphi_2^2$

For $h_2 : C_3 \to \mathrm{Aut}(C_7)$

$h_2(y) = \varphi_4$

$h_2(z) = \varphi_2 = \varphi_4^2$

Let's redo crucial calc for $C_2 \rtimes_{h_1} C_3$ using z instead of y.

$(1,z) * (x,1) = (h_1(z)(x), z) = (\varphi_4(x), z) = (x^4, z)$

so I get $ZX = X^4 Z$.

I can also describe $C_7 \rtimes_{h_1} C_3$ by generators

$\langle X, Z \ ; \ X^7 = Z^3 = 1 \ , ZX = X^4 Z \rangle$

so switching generator ~~is~~ $y \longleftrightarrow z$ in C_3 switches the descriptions $G(21) \longleftrightarrow G(21)'$

So ~~whereas~~ eventhough there are apparently 3 groups, there are only 2, up to isomorphism.

Recognition Criterion

"How can you tell whether G is a semidirect product?"

Thm: Let G be a finite group and suppose that G has subgroups K, Q with the following properties

i) K is normal in G $(K \lhd G)$

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

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

Then for some homo $h : Q \to \mathrm{Aut}(K)$ it is true that

$G \cong K \rtimes_h Q$

Before the proof need to remind you about normal subgrps.

Normality There are a number of different ways of saying this:

$K \subset G$ subgroup of G.

Defn: $\boxed{\forall g \in G \quad gK = Kg}$ (I)

In terms of elements this is equivalent to

$\boxed{\forall g \in G \quad \forall k \in K \quad gkg^{-1} \in K}$ (II)

Prop: (I) $\Leftrightarrow$ (II)

Pf: Suppose (I) Let $g \in G$, $k \in K$. Then $gk \in gK$.

But $gK = Kg$ so $gk = k_1 g$ for some $k_1 \in K$

$gkg^{-1} = k_1 \in K$ so (I) $\Rightarrow$ (II)

Suppose (II), and let $g \in G$ $gK = \{gk : k \in K\}$

$Kg = \{k'g : k' \in K\}$ If $gk \in gK$ consider gkg^{-1}

By hyp(II), $gkg^{-1} \in K$ so $gkg^{-1} = k'$ for some k'

$gk = k'g \in Kg$ so $gK \subset Kg$

If $k'g \in Kg$ $g^{-1}k'g \in K$ by hypothesis

$(g^{-1})k'(g^{-1})^{-1}$

So $k'g \in gK$ $Kg \subset gK$ so $gK \subset Kg \subset gK$ $\boxed{gK = Kg}$

SO (I) $\Leftrightarrow$ (II)

There is an even better way of thinking about normality

Suppose Q subgroup of G. Get homo: $c : Q \to \mathrm{Aut}(G)$

$c(q)(x) = qxq^{-1}$ Taking $Q = G$, $c(g)(x) = gxg^{-1}$ ← conjugation by g.

Prop: $K \lhd G$ iff for every $g \in G$, $c(g)(K) = K$, normal subgroups are "stable" under conjugation.

Proof: $c(g)(K) = gKg^{-1}$

K is normal $\Leftrightarrow gK = Kg \Leftrightarrow gKg^{-1} = K$ $\square$.

In terms of elements,

$\boxed{c(g)(k) \in K \quad \forall\, g \in G.}$ $\qquad c(g)(k) = gkg^{-1}$

so

This is what we'll use.

Prop: If $\boxed{K \triangleleft G}$ and $Q \subset G$ is a subgroup we get a homo.

$$c : Q \to \mathrm{Aut}(K)$$

$$\boxed{c(q)(k) = qkq^{-1}}$$

Algebra 4 PC sheet II 3rd Feb 2012

$D_{10} = \langle x, y \mid x^5 = y^2 = 1 \quad yx = x^4 y \rangle$

$H = \{1, y\} \qquad K = \{1, x, x^2, x^3, x^4\}$

$H \ntriangleleft D_{10} \qquad K \triangleleft D_{10}$

There are more subgroups.... $\{1\} \triangleleft D_{10} \qquad D_{10} \triangleleft D_{10}$

$\left\{ \{1, xy\} \quad \{1, x^2 y\} \quad \{1, x^3 y\} \quad \{1, x^4 y\} \right\} \ntriangleleft D_{10}$

↑ all iso to C_2.

$x\{1, xy\} = \{x, x^2 y\}$ not equal.

$\{1, xy\} x = \{x, y\}$

$g \in D_{10}$, $g D_{10} = D_{10}$

for any ~~g~~ G , $G \triangleleft G$.

$C_2 = \{1, x\} \quad C_2 = \{1, y\}$

$\mathrm{Aut}(C_2 \times C_2)$

$C_2 \times C_2 \to \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$G \xrightarrow{Y} G$

$1 \to 1$

$x \to y$

$y \to x$

$xy \to xy$

$Y^2 = 1$

$1 \to 1$

$x \to x$

$y \to y$

$xy \to xy$

X

$1 \quad 1$

$x \to xy$

$y \to x$

$xy \to y$

$X^3 = 1$

$YX = X^2 Y$

Z

④ $\mathrm{Aut}(C_2 \times C_2) \cong D_6$

City slickers method:

$C_2 \times C_2 \cong \mathbb{F}_2 \oplus \mathbb{F}_2$ $\qquad$ $\mathbb{F}_2$ field with 2 elements 0, 1.

$\mathrm{Aut}(C_2 \times C_2) \cong \mathrm{Aut}(\mathbb{F}_2^{\,2}) = \{\text{Invertible } 2\times 2 \text{ matrices}/\mathbb{F}_2\}$

$GL_2(\mathbb{F}_2)$

16 2×2 matrices$/\mathbb{F}_2$ $\qquad$ $\cancel{\begin{pmatrix}0&0\\0&0\end{pmatrix}}$

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

$\cancel{\begin{pmatrix}1&1\\0&0\end{pmatrix}} \cancel{\begin{pmatrix}1&0\\1&0\end{pmatrix}} \begin{pmatrix}1&0\\0&1\end{pmatrix}\checkmark \begin{pmatrix}0&1\\1&0\end{pmatrix}\checkmark \cancel{\begin{pmatrix}0&1\\0&1\end{pmatrix}} \cancel{\begin{pmatrix}0&0\\1&1\end{pmatrix}}$

[illegible] $\begin{pmatrix}0&1\\1&1\end{pmatrix}\checkmark \begin{pmatrix}1&0\\1&1\end{pmatrix}\checkmark \begin{pmatrix}1&1\\0&1\end{pmatrix}\checkmark \begin{pmatrix}1&1\\1&0\end{pmatrix}\checkmark$

$\cancel{\begin{pmatrix}1&1\\1&1\end{pmatrix}}$

Tick the invertible ones

$|\mathrm{Aut}(C_2 \times C_2)| = 6$

Take $x = \begin{pmatrix}0&1\\1&1\end{pmatrix}$ $\quad y = \begin{pmatrix}0&1\\1&0\end{pmatrix}$ $\quad y^2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$

$x^2 = \begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix} = x^2 \qquad x^3 = 1$

$x^2 y = \begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&1\\0&1\end{pmatrix} = yx$ $\qquad$ so $\mathrm{Aut}(C_2 \times C_2) = D_6$

$\mathrm{Aut}(C_3 \times C_3) \cong GL_2(\mathbb{F}_3) = 2\times 2$ invertible$/\mathbb{F}_3$:

$\mathrm{Aut}(C_2 \times C_3 \times C_2) \cong \underbrace{GL_3(\mathbb{F}_2)}_{168 \text{ elements}} = 3\times 3$ invertible$/\mathbb{F}_3$

Algebra 3rd Feb 2012

~~$\mathrm{Aut}(C_2 \times C_2) \cong D_6$~~

~~City slickers~~

Recognition Criterion

Let G be a finite group and suppose that

i) K, Q are subgroups of G

ii) $K \triangleleft G$

iii) $K \cap Q = \{1\}$

iv) $|K||Q| = |G|$

Then $\boxed{G \cong K \rtimes_h Q}$ for some homo $h : Q \to \mathrm{Aut}(K)$

Proof: Define $h : Q \to \mathrm{Aut}(K)$ by $\boxed{h(q)(k) = qkq^{-1}}$

Because $K \triangleleft G$, this is well defined.

h is a homomorphism.

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

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

$$\Rightarrow h(q_1 q_2)(k) = [h(q_1) \circ h(q_2)] k \text{. so homo.}$$

So $K \rtimes_h Q$ is now defined.

Define a mapping $\Phi : K \rtimes_h Q \to G$ $\qquad \Phi(k, q) = kq$ (product in G)

I claim that Φ is an isomorphism.

Got to show a) Φ is a homo b) Φ is inj c) Φ is surj

Consider $(k_1, q_1) * (k_2, q_2)$ product $K \rtimes_h Q$

$$\overset{\shortparallel}{\left(k_1 h(q_1)(k_2), q_1 q_2\right)} \text{ and apply } \Phi$$

$$\Phi[(k_1, q_1) * (k_2, q_2)] = \Phi[k_1 h(q_1)(k_2), q_1 q_2) = k_1 h(q_1)(k_2) q_1 q_2$$

$$= k_1 (q_1 k_2 q_1^{-1}) q_1 q_2 = k_1 q_1 k_2 q_2 \quad \Rightarrow \Phi[(k_1, q_1) * (k_2, q_2)] = k_1 q_1 k_2 q_2$$

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

so $\Phi[(k_1,q_1)*(k_2,q_2)] = \Phi(k_1,q_1)\,\Phi(k_2,q_2)$

ie Φ is indeed a homo $\boxed{a.}$

b) Φ inj. Suppose $\Phi(k_1,q_1) = \Phi(k_2,q_2)$

Got to show $k_1 = k_2$ and $q_1 = q_2$ $\Rightarrow k_1 q_1 = k_2 q_2$

so... $k_2^{-1} k_1 = q_2 q_1^{-1}$ ($= \eta$ say)

$$\left.\begin{array}{l} \eta = k_2^{-1}k_1 \text{ so } \eta \in K \\ \text{and } \eta = q_2 q_1^{-1} \text{ so } \eta \in Q \end{array}\right\} K, Q \text{ subgroups}$$

so $\eta \in K \cap Q$ But $K \cap Q = \{1\}$ so $\eta = 1$

$\Rightarrow k_2^{-1}k_1 = 1$ and $q_2 q_1^{-1} = 1$ $\Rightarrow k_1 = k_2$ $q_1 = q_2$ $\boxed{b}$

c) Φ surj

$\Phi : K \rtimes_h Q \longrightarrow G$ is inj.

But $|K \rtimes_h G| = |K||G| = |G|$ so Φ is an injective map between two finite sets of same cardinal, so Φ is automatically surj $\boxed{c}$

To apply Recog Crt we need to be able to find subgroups $K, Q \leq G$ s.t.

ⓔⓖ In classification of groups of order $2p$ (p odd prime) we spent a lot of time showing

$$\left.\begin{array}{l} 1) \ \exists \text{ subgrp of order } p = K \\ 2) \ \exists \text{ `` `` `` } 2 = Q \end{array}\right\} \text{ obvs } K \cap Q = \{1\}$$

what I effectively showed was that $|G| = 2p$ then $G \cong C_p \rtimes_h C_2$

so we came to

Sylow's Thm (pronounced "seal-off")

Let G be a finite group st $|G| = kp^n$

p is prime, k coprime to p, $p \nmid k$. Then

i) G has at least one subgroup of order p^n

ii) If N_p = no of sbgrps of order p^n then $N_p \equiv 1 \pmod{p}$

iii) N_p divides $|G|$ exactly.

iv) If P is subgrp $|P| = p^n$, $P' = p^m$ $m \leq n$ then $\exists g \in G$ $gP'g^{-1} \subset P$.

ⓔⓖ Sylow Counting $|G| = 15$.

$|G| = 15 = 5 \cdot 3$ go for large prime first

By Sylow, $\exists$ subgrp K, $|K| = 5$

" " " " Q, $|Q| = 3$.

N_5 = no of subgrps of order 5, $N_5 \equiv 1 \pmod{5}$

So $N_5 = 1$ or $N_5 \geq 6$

Suppose $K_1, \dots, K_6$ are subgroups $|K_i| = 5$. Each K_i has 4 elements of order 5. So G contains at least $4 \times 5 = 20$ elements $\therefore$ ✗.

So $N_5 = 1$. So K is unique subgrp of order 5. If $g \in G$, gKg^{-1} is also subgrp of order 5 so $gKg^{-1} = K$, so $K \triangleleft G$

$K \cap Q = \{1\}$ (3,5 coprime)

$|G| = |K||G|$ so

$G \cong C_5 \rtimes_h C_3$ for some $h: C_3 \to \overset{\cong C_4}{Aut(C_5)}$

So h must be trivial homo so $G \cong C_5 \times C_3 \cong C_{15}$

so $\exists$ unique group of order 15.

Algebra

7th Jan 2012

Sylow I Thm (repeated)

Suppose p prime, G finite group with $|G| = kp^n$ where $p \nmid k$

Then i) G has at least one subgrp of order p^n

ii) if N_p = no. of subgroups of order p^n then $N_p \equiv 1 \pmod{p}$

Application: Groups of order 15

G group, $|G| = 15 = 5 \times 3$

Practical Advice: Always go for large prime first

Sylow says G has

a) a subgroup K of order 5

b) a subgroup Q of order 3

Also that $N_5 \equiv 1 \pmod{5}$. So either

i) $N_5 = 1$ and $\exists$ unique subgroup of order 5 or

ii) $N_5 \geq 6$

Suppose $N_5 \geq 6$ and let $K_1, \ldots, K_6$ be distinct subgroups of order 5 (Each $K_i \cong C_5$) Each K_i has $4 = (5-1)$ elements of order 5

Also, $K_i \cap K_j = \{1\}$ otherwise $K_i \cap K_j$ would have an element of order 5 which would generate both K_i and K_j so that $K_i = K_j$ $\times$ (distinct)

So then $K_1, \ldots, K_6$ would contain $24 = 6 \times 4$ $[= 6 \times (5-1)]$ elements of order 5 $\times$ as $|G| = 15 < 24$. So supposition false

$\Rightarrow$ $\boxed{N_5 = 1}$ And K is unique subgroup of order 5

Notice that K must now be normal in G.

If $g \in G$, gKg^{-1} is also a subgrp of order 5 so $gKg^{-1} = K$ (by uniqueness)

So now we have subgroups K, Q in G.

$K \triangleleft G$ $\quad K \cap Q = \{1\}$ because $\underset{5}{|K|}$ is coprime to $\underset{3}{|Q|}$

and $$\underset{5 \times 3}{|K||Q|} = \underset{15}{|G|}$$

By recognition criterion $G \cong K \rtimes_h Q$ for some homo $h: Q \to \text{Aut}(K)$

$G \cong C_5 \rtimes_h C_3$ $h: C_3 \to \underset{\cong C_4}{\text{Aut}(C_5)}$ As 3,4 are coprime h is trivial:

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

We arrive at

<u>Thm.</u>

If $|G| = 15$ then $\exists$ $G \cong C_{15}$

ie. $\exists$ unique (up to isomorphism) group of order 15.

$g \in G$ and $K \subset G$ a subgroup

$C_g : G \to G$ $C_g(x) = gxg^{-1}$ each C_g is an auto of G. so

C_g(Any subgrp of G) = some 'other' subgroup.

Also C_g bijective so $|C_g(K)| = |K|$ so $C_g(K)$ is a subgroup with some order as K. Now if K is the unique subgroup of that order then $C_g(K) = K \Rightarrow K \lhd G$

n	Groups	Complete?	n	Groups	Complete?
1	$\{1\}$	✓	17	C_{17}	✓
2	C_2	✓	18	Slightly less messy	??
3	C_3	✓	19	C_{19}	✓
4	$C_4, C_2 \times C_2$	✓	20	$C_{20}, C_{10} \times C_2, D_{20}, D_{10}^*, G(20)$	?
5	C_5	✓	21	$C_{21}, G(21)$	✓
6	C_6, D_6	✓	22	C_{22}, D_{22}	✓
7	C_7	✓	23	C_{23}	✓
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$	? Yes but not proved	24	$\ddot{\frown}$	
9	$C_9, C_3 \times C_3$	? "			
10	C_{10}, D_{10}	✓			
11	C_{11}	✓			
12	$C_{12}, C_6 \times C_2, D_{12}, A_4, D_6^*$	?			
13	C_{13}	✓			
14	C_{14}, D_{14}	✓			
15	C_{15}	✓			
16	MESS	??			

Prop: There are exactly 2 groups of order 4; $C_4, C_2 \times C_2$

Pf: Suppose $|G| = 4$

Either i) G has an element of order 4, or

ii) $\forall g \in G \quad g^2 = 1$

If i) $G \cong C_4$

If ii) $G \cong C_2 \times C_2$ (2 lectures ago) □.

GROUPS of ORDER 21

G. $\quad |G| = 21 = 7 \cdot 3$

Sylow tells us that G has

i) a subgroup of order 7 $\quad \underline{K} \leftarrow$ Go for largest first

ii) a subgroup of order 3 $\quad Q$

$N_7 \equiv 1 \pmod 7$

So either i) $N_7 = 1$ and $K \lhd G$ or

ii) $N_7 \geq 8$

Suppose $K_1 \dots K_8$ are distinct subgroups of order 7. Remove 1 from each K_i. Each K_i has $6 = (7-1)$ elements of order 7 So G has at least $8 \times 6 = 8 \times (7-1)$ elements of order 7. Contradiction as $21 < \overset{48}{48} \Rightarrow N_7 = 1$ and $K \lhd G$

Now: Reapply Recog Crit

$K, Q \subset G \qquad K \lhd G \qquad K \cap Q = \{1\}$ 7 coprime to 3

$|G| = |K||Q| \qquad 21 = 7 \cdot 3$

So $G \cong K \rtimes_h Q = C_7 \rtimes_h C_3$ for some h.

Now we've seen there are only three homos $h : C_3 \to \mathrm{Aut}(C_7)$

$C_7 = \{1, x, \dots, x^6\} \qquad \mathrm{Aut}(C_7) = \{\varphi_1\ \varphi_2\ \varphi_3\ \varphi_4\ \varphi_5\ \varphi_6) \cong C_6$

Generator φ_3. $\qquad \varphi_3^2 = \varphi_2 \qquad \varphi_3^4 = \varphi_4$

$C_3 = \{1, y, y^2\}$ Possible homos $C_3 \to \mathrm{Aut}(C_7)$ $h_0(y) = \mathrm{Id}$ $\quad h_1(y) = \varphi_2$ order 3

$h_2(y) = \varphi_4$

Apparently 3 semidirect prods.

$h_0 : \langle X, Y \mid X^7 = Y^3 = 1 \quad YX = XY \rangle \cong C_7 \times C_3 \cong C_{21}$

$h_1 : \langle X, Y \mid X^7 = Y^3 = 1 \quad YX = X^2 Y \rangle \quad G(21)$

$h_2 : \langle X, Y \mid X^7 = Y^3 = 1 \quad YX = X^4 Y \rangle \quad G'(21$

Switching $y \leftrightarrow y^2$ gives $G(21) \cong G'(21)$

$\Rightarrow$ Only 2 groups of order 21.

GROUPS of ORDER 20

G finite group, $|G| = 20 = 5 \cdot 2^2$

i) G has a subgrp of order 5 K

ii) " " " 4 Q

Case I $Q = C_4$

Case II $Q = C_2 \times C_2$

However, in either case $K \lhd G$

$N_5 \equiv 1 \pmod 5$ so either

a) $N_5 = 1$ and $K \lhd G$ or

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

Contradiction: So $N_5 = 1$ & $K \lhd G$.

We now apply Recognition Crit to get

$$G \cong K \rtimes_h Q \cong C_5 \rtimes_h Q \quad \text{where } h : Q \to \mathrm{Aut}(C_5) \cong C_4.$$

Case I: $Q = C_4$

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

$\mathrm{Aut}(C_5) = \{\mathrm{Id}, \varphi_2, \varphi_4, \varphi_3\}$ $\quad \varphi_2(x) = x^3 \quad \varphi_3(x) = x^3 \quad \varphi_4(x) = x^4$

$\varphi_2^2 = \varphi_4 \quad \varphi_2^3 = \varphi_3$

order $\varphi_2 = 4$ ($=$ order φ_3)

order $\varphi_4 = 2$

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

Therere are 4 homos $C_4 \to \mathrm{Aut}(C_5)$

$h_0 : C_4 \to \mathrm{Aut}(C_5)$ trivial $\quad h_0(y) = Id$

$h_1 : C_4 \to \mathrm{Aut}(C_5) \quad h_1(y) = \varphi_2 \quad h_1(y)(x) = x^2$

$h_2 : C_4 \to \mathrm{Aut}(C_5) \quad h_2(y) = \varphi_4 \quad h_2(y)(x) = x^4 (= x^{-1})$

$h_3 : C_4 \to \mathrm{Aut}(C_5) \quad h_3(y) = \varphi_3 \quad h_3(y)(x) = x^3$

$h_0 : \langle X, Y \mid X^5 = Y^4 = 1 \;, YX = XY \rangle \cong C_5 \times C_4 \cong C_{20}$ ⓪

$C_5 \rtimes_{h_1} C_4$
$h_1 : \langle \text{''} \quad \text{''} \quad \text{''} \quad YX = X^2 Y \rangle \quad G(20)$ ①

$C_5 \rtimes_{h_2} C_4$
$h_2 : \langle \text{''} \quad \text{''} \quad \text{''} \quad YX = X^4 Y$ or $YXY^{-1} = X^{-1} \rangle \quad D_{10}^*$ ②

$C_5 \rtimes_{h_3} C_4$
$h_3 : \langle \text{''} \quad \text{''} \quad \text{''} \quad YX = X^3 Y \rangle$ ③

Show ① $\cong$ ③ By switching $y \leftrightarrow y^3$ generators of C_4

Binary Dihedral Groups

D^*_{2n} has $4n$ elements. Given by generators X, Y.

$X^n = 1 \quad Y^4 = 1 \quad , \quad YXY^{-1} = X^{-1}$

If we had $Y^2 = 1$ we'd have D_{2n} but here $Y^4 = 1$

In D^*_{2n} although Y has order 4, it acts as automorphism of order 2 on $\{1, X, \dots, X^{n-1}\}$

In $G(20)$ Y has order 4 and acts with order 4 on $\{1, X, \dots, X^4\}$

exercise: $D^*_{10} \not\cong G(20)$ [Count orders of elements]

So CASE I gives three distinct groups: $C_{20}, D^*_{10}, G(20)$

Case II

$Q = C_2 \times C_2$

$G \cong C_5 \rtimes_h (C_2 \times C_2)$ for some homo $h : C_2 \times C_2 \to Aut(C_5)$

$C_5 = \{1, x, \dots, x^4\}$ $\quad Aut(C_5) = \{1, \varphi_2, \underset{\varphi_4}{\underset{\shortparallel}{\varphi_2^{\,2}}}, \underset{\varphi_3}{\underset{\shortparallel}{\varphi_2^{\,3}}}\}$

$C_2 \times C_2 = \{1, s, t, st\}$ $\quad s^2 = t^2 = 1 \quad ts = st \quad (st)^2 = 1.$

$h : C_2 \times C_2 \to Aut(C_5)$

Can't hit either $\overset{\text{order } 4}{\boxed{\varphi_2 \text{ (generator) or } \varphi_2^{\,3} = \varphi_3}}$ So either $h(s) = 1$ or $h(s) = \varphi_4$ and likewise either $h(t) = 1$ or $h(t) = \varphi_4$

Four Possibilities

$h_0(s) = 1 \quad h_0(t) = 1 \quad h_0(st) = 1 \; [= h_0(s) h_0(t)]$ Trivial

$h_1(s) = \varphi_4 \quad h_1(t) = 1 \quad h_1(st) = \varphi_4 \; [= h_1(s) h_\varphi(t)]$

$h_2(s) = 1 \quad h_2(t) = \varphi_4 \quad h_2(st) = \varphi_4$

$h_3(s) = \varphi_4 \quad h_3(t) = \varphi_4 \quad h_3(st) = 1 \; [= h_3(s) h_3(t)]$

Now work out the relations for each h,

$h_0 : \langle X, S, T \mid X^5 = S^2 = T^2 = 1, \; TS = ST, \; SX = XS, \; TX = XT \rangle$

$\cong C_5 \times C_2 \times C_2 \cong C_{10} \times C_2$

$h_1 : \langle S, X, T \mid X^5 = S^2 = T^2 = 1, \; TS = ST, \; SX = X^4 S, \; TX = XT \rangle$

$\left[\begin{array}{lll} h_1(s)(x) = \varphi_4(x) = x^4 & SXS^{-1} = X^4 & SX = X^4 S \\ h_1(t)(x) = Id(x) = x & TX = XT. & \end{array}\right]$

$\cong D_{10} \times C_2 \qquad D_{10} = \langle X, S \rangle \qquad C_2 = \langle T \rangle$

$h_2 : \langle X, S, T \mid X^5 = S^2 = T^2 = 1, \; TS = ST, \; SX = XS, \; TX = X^4 T \rangle$

$\cong D_{10} \times C_2 \qquad D_{10} = \langle X, T \rangle \qquad C_2 = \langle S \rangle$

$h_3 : \langle X, S, T \mid X^5 = S^2 = T^2 = 1, \; TS = ST, \; SX = X^4 S \quad (ST)X = X(ST) \rangle$

$D_{10} \times C_2 \qquad D_{10} = \langle X, S \rangle \qquad C_2 = \langle ST \rangle$

In Case II got 2 ~~seperate~~ distinct groups

$$C_5 \times C_2 \times C_2 \cong C_{10} \times C_2$$

$$D_{10} \times C_2 \cong D_{20}$$

So we arrive at

<u>Thm</u>: There are precisely 5 groups of order 20;

C_{20}	$C_{10} \times C_2$	D_{20}	D_{10}^*	$G(20) = \mathrm{Aff}(\mathbb{F}_5)$
$\shortparallel$	$\shortparallel$	$\shortparallel$		
$C_5 \times C_4$	$C_5 \times C_2 \times C_2$	$D_{10} \times D_2$		

Algebra (PC) sheet 3

10th Feb 2012

$\mathcal{O}_G = \{$bijective mapping $G \to G\}$

$\lambda_g : G \to G$ $\qquad \lambda_g(h) = gh$

$g \mapsto \lambda_g$ is a homomorphism $G \to \mathcal{O}_G$ $\qquad$ Using table:

$$\lambda_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} \qquad \lambda_x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

$$\lambda_{x^2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix} \qquad \lambda_{x^3} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 8 & 5 & 6 & 7 \end{pmatrix}$$

$$\lambda_y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 & 1 & 4 & 3 & 2 \end{pmatrix}$$ ..... etc. write out 8 permutations

$|G| = n$ $\qquad G \subset \mathcal{O}_n$ permutations on $\{1, \dots, n\}$

Algebra 10th Feb 2012

Groups acting on sets

G group, X set. By a *left action* of G on X we mean a mapping $*: G \times X \longrightarrow X$ written $*(g,x) = g * x$

Such that i) $\forall g,h \in G$ $\forall x \in X$ $\boxed{(gh) * x = g * \{h * x}$
product in G

ii) $\forall x \in X$ $\boxed{1 \cdot x = x}$

A right action would be a mapping : $X \times G \longrightarrow X$

$$\begin{cases} x*(gh) = (x*g)*h \\ x \cdot 1 = x \end{cases}$$

eg (Left translation)
Take $X = G$ and take $*$ = group multiplication

Cayleys Thm

Let G be a group $|G| = n$. Then G is isomorphic to a subgroup of $\sigma_n = \{$permutations on $\{1, \ldots n\}\}$

Pf: Let $\sigma_G = \{$permutations on $G\}$ $G \to G$ bijective
σ_G is a group under composition. I have a mapping
$\lambda : G \to \sigma_G$ $\lambda_g(h) = gh$ (product on G)
$g \longmapsto \lambda_g$

Each λ_g is a bijective mapping. In fact $\lambda_g^{-1} = \lambda_{g^{-1}}$

$$(\lambda_{g^{-1}} \circ \lambda_g)(x) = \lambda_{g^{-1}}(\lambda_g(x)) = \lambda_{g^{-1}}(gx) = g^{-1}(gx) = (g^{-1}g)x = x$$

$\lambda_{g^{-1}} \circ \lambda_g = \mathrm{Id}.$

Moreover: $g \longmapsto \lambda_g$ is a homomorphism.

$\lambda_{gh}(x) = (gh)x = g(hx) = \lambda_g(\lambda_h(x))$ so $\lambda_{gh} = \lambda_g \circ \lambda_h$

Finally: $g \longmapsto \lambda_g$ is injective.

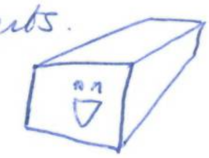
If $\lambda_g = \lambda_h$ then $\lambda_g(1) = \lambda_h(1) \Rightarrow g \cdot 1 = h \cdot 1 \Rightarrow g = h$

So $\lambda_g : G \to \mathcal{O}_G$ is an injective homomorphism.

$\lambda_g(G) \cong G \qquad (\mathrm{Im}\,\lambda_g \cong G)$

To get statement as advertised count elements.

$\langle g_1, \dots, g_n \rangle$ and replace $\mathcal{O}_G$ by $\mathcal{O}_n$



C_4

	1	x	x^2	x^3
1	1	x	x^2	x^3
x	x	x^2	x^3	1
x^2	x^2	x^3	1	x
x^3	x^3	1	x	x^2

λ_g top row = input

ρ_g left column = input

Alternative way: Mlutiply on the right.

$\rho_g(x) = xg$ ✗ wrong.

Difficulty here is you don't get a homomorphism.

$$\rho_{gh}(x) = x(gh) = (xg)h = \rho_g(x)h = \rho_h \rho_g(x)$$

we get $\rho_{gh} = \rho_h \rho_g$

Correct Defn: $\rho_g(x) = xg^{-1}$

Then $\rho_{gh} = \rho_g \rho_h$ is a homomorphism

Bettr eg: Take $X = G$ $\quad * : G \times X \to X$

$\boxed{g * x = gxg^{-1}}$ conjugation.

Get a new homomorphism $c : G \to \mathcal{O}_G (= \mathcal{O}_X)$, $\boxed{c_g(x) = gxg^{-1}}$

$$c_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = c_g(hxh^{-1}) = c_g \circ c_h(x)$$

$\boxed{c_{gh} = c_g \circ c_h}$

Alternative way of thinking about a group action:

$$* : G \times X \to X$$

$$(g, x) \longmapsto g * x$$

Alternative...

$$\pi : G \longrightarrow \sigma_x = \{\text{Permutations on } X\}$$

$$\pi(g)(x) = g * x$$

π is a homomorphism $\Leftrightarrow$ $*$ is a left action.

Orbits under group action:

Suppose $* : G \times X \to X$ is a left action. Let $x \in X$

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

$\langle x \rangle$ is called the orbit of x under G.

ⓔⓖ $G = D_6$ acting on itself by conjugation

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

$* : G \times G \longrightarrow G$ $\boxed{g * h = ghg^{-1}}$

Let's take each $h \in G$ in turn and find its orbit.

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

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

$y x y^{-1} = x^2 y y^{-1} = x^2$

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

$\langle x^2 \rangle = \{x^2, x^4\}$ $x^a x^2 x^{-a} = x^2$

$= \{x, x^2\}$ $(x^a y) x^2 (x^a y)^{-1} = x^4$

$= \langle x \rangle$

$\langle y \rangle = \{y, xy, x^2y\}$ $y y y^{-1} = y$

$x y x^{-1} = x y x^2 = x x y = x^2 y$

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

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

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

Three distinct orbits.
$\langle 1 \rangle = \{1\}$
$\langle x \rangle = \{x, x^2\}$
$\langle y \rangle = \{y, xy, x^2y\}$
$1, x, y$ is a set of orbit representatives

General Observation

Let $* : G \times X \rightarrow X$ be a left action and let $x, x' \in X$

Then either i) $\langle x \rangle \cap \langle x' \rangle = \emptyset$

or ii) $\langle x \rangle = \langle x' \rangle$

Pf: It suffices to show that if $\langle x \rangle \cap \langle x' \rangle \neq \emptyset$ then $\langle x \rangle = \langle x$

Suppose $\langle x \rangle \cap \langle x' \rangle \neq \emptyset$

ie $\exists\, z \in \langle x \rangle \cap \langle x' \rangle$

'$z \in \langle x \rangle$' means $z = g * x$ for some $g \in G$

'$z \in \langle x' \rangle$' means $z = h * x'$ for some $h \in G$

So $g * x = h * x'$ for some $g, h \in G$ SO...

$x = (g^{-1}h) * x'$ so for each $\gamma \in G$

$\langle x \rangle \Rightarrow \gamma * x = (\gamma g^{-1} h) * x' \in \langle x' \rangle$

However $\langle x \rangle = \{\gamma * x : \gamma \in G\}$ so $\langle x \rangle \subset \langle x' \rangle$

Reverse the argument $x' = (h^{-1}g) * x$ so for all $\gamma \in G$,

$\gamma * x' = (\gamma h^{-1} g) * x$ ie $\langle x' \rangle \subset \langle x \rangle$

If $\langle x \rangle \cap \langle x' \rangle \neq \emptyset$ then $\langle x \rangle \subset \langle x' \rangle \subset \langle x \rangle$

so $\langle x \rangle = \langle x' \rangle$ $\square$.

Class Equation (Version I)

G acting finite set X.

Let $x_0, \ldots, x_n \in X$ represent the distinct orbits.

$$X = \bigcup_{i=1}^{m} \langle x_i \rangle \qquad \langle x_i \rangle \cap \langle x_j \rangle = \phi \quad (i \neq j)$$

No double counting.

$$|X| = \sum_{i=1}^{m} |\langle x_i \rangle|$$

ⓔⓖ D_6 acting on itself by conjugation.

$|D_6| = 6$ $\qquad$ $1, x, y$ orbit reps.

$$D_6 = \langle 1 \rangle \cup \langle x \rangle \cup \langle y \rangle$$

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

$$|D_6| = |\langle 1 \rangle| + |\langle x \rangle| + |\langle y \rangle| = 1 + 2 + 3 = 6.$$

Algebra

21st Feb 2012

$\cdot : G \times X \to X$ (left) group action of G on X

If $x \in X$ the orbit $\langle x \rangle$ of x $\langle x \rangle = \{g \cdot x : g \in G\}$

I showed that if $x, y \in X$ either $\langle x \rangle = \langle y \rangle$ or $\langle x \rangle \cap \langle y \rangle = \emptyset$

Take elements $x_1, \dots, x_m$ in X representing the distinct orbits (set of orbit representatives)

prototype: $\boxed{X = \langle x_1 \rangle \sqcup \langle x_2 \rangle \sqcup \dots \sqcup \langle x_m \rangle}$ ← SET THEORETIC CLASS EQN

$\sqcup$ = disjoint union.

Take cardinals, get

$$\boxed{|X| = \sum_{i=1}^{m} |\langle x_i \rangle|}$$ ← CLASS EQN MARK ONE

We need to improve on this.

Let $\cdot : G \times X \to X$ group action. Let $x \in X$ define

$\boxed{G_x = \{g \in G : g \cdot x = x\}}$ ← The Stability group of x

Prop: G_x is a subgroup of G

Proof: Let $g, h \in G_x$ $g \cdot x = x$ $h \cdot x = x$ then

$(g \cdot h) \cdot x = g(h \cdot x) = gx = x \Rightarrow gh \in G_x$ so G is a closed set

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

If $g \in G_x$ $(gx = x)$ $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = x \Rightarrow g^{-1} \in G_x$

so G_x is a subgroup of G $\square$.

Prop: For each $x \in X$ i) $\exists$ a bijective mapping $G/G_x \xrightarrow{\simeq} \langle x \rangle$

ii) Hence $|\langle x \rangle| = |G|/|G_x|$

Proof $i \Rightarrow ii$ is clear, so ETP (suffices to prove) i.

First recall that

$G/G_x = \{h \cdot G_x : h \in G\}$

Recall Rule of Equality for Cosets.

$h_1 G_x = h_2 G_x \iff h_2^{-1} h_1 \in G_x$

Define $\psi : G/G_x \longrightarrow \langle x \rangle$ by $\psi(h \cdot G_x) = hx$

Need to check that ψ is well defined, ie suppose $h_1 G_x = h_2 G_x$. Got to show $h_1 x = h_2 x$

So suppose $h_1 G_x = h_2 G_x$ so $h_2^{-1} h_1 \in G_x$ so $(h_2^{-1} h_1) x = x$

So $h_2 (h_2^{-1} h_1) x = h_2 x$ so $h_1 x = h_2 x$ ie ψ is well defined.

ψ is obviously surjective

If $hx \in \langle x \rangle$ then $hx = \psi(h \cdot G_x)$

To conclude I need to show ψ is injective.

Suppose $\psi(h_1 G_x) = \psi(h_2 G_x)$

so $h_1 x = h_2 x$

so $h_2^{-1} h_1 x = x \Rightarrow h_2^{-1} h_1 \in G_x$

so $h_1 G_x = h_2 G_x$ $\square$ (injective) $\Rightarrow \square$

Numerical Class ~~[illegible]~~ eqn Mark One

$$|X| = \sum_{i=1}^{m} |\langle x_i \rangle| \qquad \text{But } |\langle x_i \rangle| = \frac{|G|}{|G_x|}$$ so substitute to get

Numerical Class eqn Mark Two.

$$|X| = \sum_{i=1}^{m} \frac{|G|}{|G_{x_i}|}$$ where $x_1 \ldots x_m$ is a set of coset representations.

Fixed Point Sets

Let $\cdot : G \times X \to X$ be a group action.

$x \in X$ is said to be a fixed point when $\boxed{gx = x}$ $\forall g \in G$

ie x is fixed $\iff G_x = G$

$X^G = \{x \in X : \forall g \in G \quad g \cdot x = x\}$

X^G is the fixed point set under action.

<u>Thm</u>: Let p be a prime and let P be a group of order p^n acting on a finite set X; then $\boxed{|X| \equiv |X^P| \pmod{p}}$

<u>Proof</u>: ~~A fixed point~~ Let $x \in X$. x is a fixed point $\Leftrightarrow \langle x \rangle = \{x\}$

Let $x_1 \dots x_m$ be a collection of orbit representatives, chosen in such a way that the fixed points come first.

$X^P = \{x_1 \dots x_k\}$ Recurring orbits represented by $\{x_{k+1}, \dots, x_m\}$

Write down the Class Eqn

$$|X| = \sum_{i=1}^{k} |\langle x_i \rangle| + \sum_{i=k+1}^{m} |\langle x_i \rangle| \qquad |\langle x_i \rangle| = 1 \text{ for } 1 \leq i \leq k$$

$$|\langle x_i \rangle| = |P| / |P_k| > 1 \quad \text{for } k+1 \leq i \leq m$$

$$|X| = k + \sum_{i=k+1}^{m} |P| / |P_k| \qquad k = |X^P|$$

$$|P| = p^n \qquad |P_k| = p^{e_i} \quad \text{for some } e_i \quad e_i < n.$$

$$|X| = k + \sum_{i=k+1}^{m} p^{n-e_i} \qquad n - e_i \geq 1$$

So p divides $\sum_{i=k+1}^{m} p^{n-e_i}$ So mod p.

$|X| \equiv k \equiv |X^P| \pmod{p}$ □

Corollary (Wilson's Thm)

Let p be a prime, and $k \geq 1$ an integer

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

nomial eff $\nearrow$

Proof: Let P be some group of order p^n (It doesn't matter which one) Let $X = \underset{\text{times}}{\overset{\nearrow}{P}} \times \{1, \dots, k\}$. Define

$\bullet : P \times X \longrightarrow X$ by $g \bullet (h, r) = (gh, r)$ left action.

Let $\mathcal{X} = \{A \subset X : |A| = p^n\}$ $\quad |\mathcal{X}| = \binom{kp^n}{p^n}$

$|X| = kp^n$ taking subsets of order p^n so get $\binom{kp^n}{p^n}$ such subsets!

Let P act on $\mathcal{X}$ as follows.

$$* : P \times \mathcal{X} \rightarrow \mathcal{X}$$

$g * A = \{ga : a \in A\} = gA$

so $|\mathcal{X}| \equiv |\mathcal{X}^P| \pmod p$ by above.

Need to find $\mathcal{X}^P$.

Let $A \subset P \times \{1 \dots k\}$ be such that $g \cdot A = A$ $\forall g \in G$ and $|A| = p^n$.

Let $a \in A$. $a = (h, r)$

$g \cdot a = (gh, r)$ $\curvearrowright$ represents arbitrary element of P.

so $P \times \{r\} \subset A$ but $|P \times \{r\}| = |A| = p^n$. So a fixed point of $\mathcal{X}$ is precisely a set $P \times \{r\}$ $r = 1 \dots k$. There are k such sets.

So $|\mathcal{X}^P| = k$

However $|\mathcal{X}| = \binom{kp^n}{p^n}$ so $\binom{kp^n}{p^n} \equiv k \pmod p$ $\square$.

Sylow's Thm (Part One)

Let G be a finite group. $|G| = kp^n$, p prime and $p \nmid k$. Then G has at least one subgroup P with $|P| = p^n$.

Proof: By induction on k.

For $k=1$ there is nothing to prove. $P = G$.

Suppose proved for groups of order $k'p^n$ where $k' < k$, and let $|G| = kp^n$. Let $\mathcal{A} = \{A : A \text{ is a subset of } G \text{ and } |A| = p^n\}$

So $|\mathcal{A}| = \binom{kp^n}{p^n}$ By A-level.

Consider the following action. $G \times \mathcal{A} \to \mathcal{A}$

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

Take the class eqn.......

$$|\mathcal{A}| = \sum_{i=1}^{\nu=\text{WHEREVER MAN}} \frac{|G|}{|G_{A_i}|}$$ where $A_1 \dots A_r$ is a set of orbit reps

$|G| = kp^n$ $\quad |G_{A_i}| = k_i p^{e_i}$ for some k_i dividing k, $e_i \leq n$

By Lagrange ↗

$$|\mathcal{A}| = \binom{kp^n}{p^n} \quad \text{so} \quad \binom{kp^n}{p^n} = \sum_{i=1}^{\nu} \left(\frac{k}{k_i}\right) p^{n-e_i}$$

We've shown that $\binom{kp^n}{p^n} \equiv k \pmod{p}$

So p doesn't divide LHS, so p doesn't divide RHS.

However if each $e_i < n$ then p does divide RHS, so for some i, $\boxed{|G_{A_i}| = k_i p^n}$

Claim that $k_i < k$, otherwise if $k_i = k$ then $G_{A_i} = G$ so A_i is fixed under the action. If $a \in A_i$ get an injective mapping

$$\begin{array}{l|l} G \longrightarrow A_i & \text{Contradiction as } |G| = kp^n \text{ but } |A_i| = p^n \\ g \longmapsto ga & \text{and } kp^n > p^n. \end{array}$$

So $k_i < k$, $|G_{A_i}| = k_i p^n$. By induction, G_{A_i} has a subgroup P, with $|P| = p^n$. So P is also a subgroup of G, and $|P| = p^n$ $\square$.

The full Sylow Thm says this:

① If $|G| = kp^n$ $p \nmid k$ then G has at least one subgroup P with $|P| = p^n$

② If N_p = no. of subgroups of order p^n then $N_p \equiv 1 (\mathrm{mod}\, p)$ Next lecture.

③ N_p divides $|G|$ (won't prove)

④ If P' is a subgroup of order p^m and $(m<n)$ then $\exists$ P, a subgroup of order p^n such that $P' \subset P$ (won't prove)

Quotient Groups

Suppose G group and K is a normal subgroup ($K \triangleleft G$). We'll show that the set G/K is naturally a group.

subk) $G/K = \{gK : g \in G\}$ $\qquad g_1K = g_2K \Leftrightarrow g_2^{-1}g_1 \in K$

$$\boxed{K \triangleleft G \text{ means } \forall g \in G \quad gKg^{-1} = K}$$

Defn: Suppose $K \triangleleft G$. Define $* : G/K \times G/K \to G/K$ by $(g \cdot K) * (hK) = (gh)K$.

Prop: If $K \triangleleft G$ then $* : G/K \times G/K \longmapsto G/K$ is well defined and gives a group multiplication on G/K

Proof: Need to show that if $g_1K = g_2K$ and $h_1K = h_2K$ then $(g_1h_1)K = (g_2h_2)K$ ie. if $g_2^{-1}g_1 \in K$ and $h_2^{-1}h_1 \in K$ then $(g_2h_2)^{-1}(g_1h_1) \in K$.

But $(g_2h_2)^{-1}(g_1h_1) = h_2^{-1}g_2^{-1}g_1h_1 = \underbrace{[h_2^{-1}g_2^{-1}g_1h_2]}_{\in_K}(h_2^{-1}h_1)$

Now $g_2^{-1}g_1 \in K$ so

$$\underset{\cap_K}{h_2^{-1}(g_2^{-1}g_1)h_2} = (h_2^{-1})(g_2^{-1}g_1)(h_2^{-1})^{-1} \qquad K \triangleleft G.$$

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

so $g_1K = g_2K$ and $h_1K = h_2K \Rightarrow (g_1h_1)K = (g_2h_2)K$ and product is well defined.

Assoc: Obvious

$$(gK)[(hK)(lK)] \quad (gK)(hlK) = g(hl)K = [(gh)l]K = (ghK)(l$$

$$= [(gK)(hK)](lK$$

Identity: $1 \cdot k = k$

Inverse: $(gk)^{-1} = g^{-1}k$

~~[illegible]~~ Algebra

24th Feb 2012

G group. K normal subgroup of G. $K \triangleleft G$.

$$\boxed{\forall g \in G \quad \forall k \in K \quad gkg^{-1} \in K}$$

$$* : G/K \times G/K \longrightarrow G/K$$

$(gK) * (hK) = ghK$ well defined (only because)

This gives a group ~~structure~~ multiplication on G/K

Assoc: $(gK) * [(hK) * (lK)] = (gK) * (hlK) = g(hl)K = (gh)lK$

$= (ghK) * (lK) = [(gK) * (hK)] * (lK)$

Identity: $1 \cdot K = K$ 1 is the Id.

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

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

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

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

So G/K is a group when $K \triangleleft G$ $\square$.

ⓔⓖ $G = Q_8$

$G = \{1, -1, i, -i, j, -j, k, -k\}$ $K = \{1, -1\} \triangleleft G$ $|K| = 2$

Question: Which group is G/K?

So $\left| G/K \right| = 8/2 = 4$ Two possibilities: C_4, $\boxed{C_2 \times C_2}$?

$\Rightarrow Q_8/\{\pm 1\} \cong C_2 \times C_2$ The elements of $Q_8/\{\pm 1\}$ are ... continued at end

Defn: Let H, Q be subgroups of G

Say that Q normalises H when $\boxed{\forall q \in Q \ \forall h \in H \ \ qhq^{-1} \in H}$

Prop: If Q normalises H then

$HQ = \{hq : h \in H, q \in Q\}$ is a subgroup of G, and $H \lhd HQ$

proof: Need to show

i) HQ closed w.r.t multiplication

ii) $1 \in HQ$

iii) if $x \in HQ$ then $x^{-1} \in HQ$

---

i) Let $x, y \in HQ$ so $x = h_1 q_1 \quad y = h_2 q_2$

Then $xy = h_1 q_1 h_2 q_2 = (h_1 q_1 h_2 q_1^{-1})(q_1 q_2)$

But $q_1 h_2 q_1^{-1} \in H$ (Normalisation Condition)

so $h_1 q_1 h_2 q_1^{-1} \in H \quad q_1 q_2 \in Q \quad$ so $xy \in HQ$

ii) $1 = 1 . 1 \quad 1 \in H \quad 1 \in Q \quad$ QED.

iii) Let $x \in HQ \quad x = hq \quad$ Then $x^{-1} = (hq)^{-1} = q^{-1}h^{-1}$

$q^{-1}h^{-1} = (q^{-1}h^{-1}q)q^{-1} \quad q^{-1}h^{-1}q \in H \quad q^{-1} \in Q \Rightarrow x^{-1} \in HQ.$

So HQ is a subgroup of G.

Claim $H \lhd HQ$.

Let $h \in H \quad y \in HQ \quad$ got to show $yhy^{-1} \in H$

Write $y = h_1 q_1 \quad y^{-1} = q_1^{-1} h_1^{-1} \quad yhy^{-1} = h_1(q_1 h q_1^{-1})h_1^{-1}$

But $q_1 h q_1^{-1} \in H$ so $h_1(q_1 h q_1^{-1})h_1^{-1} \in H$ QED.

et H, Q be subgroups of G and Q normalises H. so $H \lhd HQ$

Question: What is HQ/H?

E - Noethers 1st Isomorphism Thm

~~Noether's~~ Let H, Q be subgroups of G. Suppose Q normalises H.

Then $\boxed{HQ/H \cong Q/H\cap Q}$

<u>Proof</u>: Define $\nu : Q \longrightarrow HQ/H$ by $\nu(q) = qH \; (= 1 \cdot q \cdot H)$

ν is a homo.

$\nu(q_1 q_2) = q_1 q_2 H = (q_1 H)(q_2 H) = \nu(q_1)\nu(q_2)$

ν is surjective. Why?

An arbitrary element of HQ/H looks like $hqH = qq^{-1}hqH$

But $q^{-1}hq \in H$ so $q^{-1}hqH = H$

so arbitrary element $hqH \in HQ/H$ is in fact $qH = \nu(q)$

s. ν is surjective.

$\nu : Q \longrightarrow HQ/H$ is surjective. So $\mathrm{Im}(\nu) = HQ/H$

ν_* induces a bijection.

$$\nu_* : \frac{Q}{\mathrm{Ker}(\nu)} \longrightarrow \mathrm{Im}(\nu)$$

Question: What is $\mathrm{Ker}(\nu)$? $\mathrm{Ker}(\nu) = \{ q \in Q : qH = H \}$

But $qH = H$ iff $q \in H$

so $\mathrm{Ker}(\nu) = H \cap Q$ so we have a bijection.

$$\nu_* : \frac{Q}{H \cap Q} \longrightarrow \frac{HQ}{H}$$ This is a group isomorphism □

Noethers 0^A Iso Thm

If $\alpha : G \to H$ homo

$\alpha_* : \frac{G}{\mathrm{Ker}(\alpha)} \longrightarrow \mathrm{Im}(\alpha)$ is an iso

Sylow part II

Let G be a group $|G| = kp^n$, p prime, $p \nmid k$.

$N_p = \{$no of subgroups of order $p^n\}$ Then $N_p \equiv 1 \pmod{p}$

Proof: Put $\mathcal{P} = \{ \varphi : P$ is a subgroup of G $|P| = p^n \}$

Know $\mathcal{P} \neq \emptyset$ (Sylow part I)

Let $P \in \mathcal{P}$ be a specific subgroup $|P| = p^n$

Let P act on $\mathcal{P}$

$* : P \times \mathcal{P} \longrightarrow \mathcal{P}$

$g * H = gHg^{-1}$ $\quad$ gHg^{-1} is also a subgroup of order p^n

$\mathcal{P}^P = \{ H \in \mathcal{P} : \forall g \in P \quad gHg^{-1} = H \}$

$= \{$ subgroups in $\mathcal{P}$ which are normalised by $P \}$

Since $|P| = p^n$ I know

$|\mathcal{P}| = |\mathcal{P}^P| \pmod{p}$ so $|\mathcal{P}| = N_p$.

To complete proof I just need to ~~know~~ show that

$|\mathcal{P}^P| = 1$ $\quad (N_p \equiv 1 \pmod{p})$

Clearly P normalises itself so $P \in \mathcal{P}^P$

Suppose $H \in \mathcal{P}^P$ so P normalises H. So HP is a subgroup of G.

and $\frac{HP}{H} = \frac{P}{H \cap P}$ so $|HP| = \left| \frac{P}{H \cap P} \right| |H|$

$|P| = p^n$ so $\left| \frac{P}{H \cap P} \right| = p^m$ for some m $\quad 0 \leq m < n$.

$|H| = p^n$ so $|HP| = p^{n+m}$ HP is a subgroup of G.

$|G| = kp^n$ $\quad p \nmid k$

So p^{n+m} divides kp^n $\quad p \nmid k \quad$ so $m=0$

and $\left|P/_{H\cap P}\right| = 1 \quad$ ie $\quad H \cap P = P$

so $\quad |HP| = p^n \quad$ Now $\quad H \subset HP$ and $|H| = p^n$

so $\quad H = HP \quad$ But $\quad P \subset HP \quad |P| = p^n$

so $\quad P = HP = H \quad$ and I've shown that

P is the element of $\mathcal{P}$ fixed under the action of P.

ie $\quad |\mathcal{P}^P| = 1 \quad$ and $\quad N_p \equiv 1 \bmod p \quad \square$

<u>continued</u>: $\quad Q_8/_{\{\pm 1\}} \cong C_2 \times C_2$

The elements of this are $\underset{K}{\{1,-1\}} \quad \underset{iK}{\{i,-i\}} \quad \underset{jK}{\{j,-j\}} \quad \underset{kK}{\{k,-k\}}$

$(iK)^2 = i^2K = (-1)K = K$

$(jK)^2 = j^2K = (-1)K = K$

$(kK)^2 = (-1)K = K$

so $\forall g \in Q_8/_{\{\pm 1\}} \quad g^2 = 1 \qquad Q_8/_{\{\pm 1\}} \cong C_2 \times C_2$

Algebra 28th Feb 2012

$* : X \times X \to X$ "multiplication"

Usually want $*$ to be associative.

A $\boxed{\text{semigroup}}$ is a pair $(X,*)$, $*$ is associative.

Next need Id ie specific $e \in X$

$$e*x = x = x*e \quad \forall x \in X.$$

A $\boxed{\text{monoid}}$ is triple $(X,*,e)$ $*$ is associative, e identity

Next we need inverses $\forall x \in X \ \exists x^{-1} \in X$ st $x * x^{-1} = e$

$$x^{-1} * x = e$$

A $\boxed{\text{group}}$ is a triple $(X,*,e)$ where $*$ assoc, e identity, inverses exist

Next stage involves taking two structures in same set.

RINGS

Defn: By a ring R we mean $R = (R, +, 0, \cdot, 1)$ (5-tu

where i) $(R,+,0)$ is an abelian group, $x+y = y+x$

ii) $(R, \cdot, 1)$ is a monoid

iii) $0 \neq 1$

iv) $\forall x,y,z \in R$ $\begin{cases} x \cdot (y+z) = xy + xz \\ (y+z)x = yx + zx \end{cases}$ DISTRIBUTIVE LAWS

(Rings don't expect to have inverses)

A ring R is said to be COMMUTATIVE when

$$\forall x,y \in R \quad \boxed{x*y = y*x}$$

Usually we'll consider only commutative rings, however...

(egs) i) $\mathbb{Z}$ is a commutative ring.

ii) $\mathbb{Q}$ is a ring aswell as a field

iii) $\mathbb{R}$ " " " " "

iv) $\mathbb{C}$ " " " "

Defn A division ring D is a ring with an extra property.

$$\boxed{\forall x \in D,\ x \neq 0\ \exists x^{-1} \in D\ ;\ xx^{-1} = 1 = x^{-1}x}$$

A commutative division ring is called a field.

$\mathbb{H}$ = Hamiltonian quaternions.

$\mathbb{H}$ is vector space over $\mathbb{R}$ of dimension 4, $1, i, j, k$

$a_0 1 + a_1 i + a_2 j + a_3 k \qquad a_i \in \mathbb{R}$

where $i^2 = j^2 = k^2 = -1$

$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$

First ever noncommutative division ring.

f R ring, $M_n(R)$ = $n \times n$ matrices $/R$

$M_n(R)$ is a noncommutative ring when $n \geq 2$

$\mathbb{Z}$ is a ring but not a field. Because $2^{-1} = \frac{1}{2} \notin \mathbb{Z}$

More examples

n integer $n > 1$ INFORMAL DEFN.

$\mathbb{Z}/_n$ ($\mathbb{Z}$ mod n). $\mathbb{Z}/_n = \{0, 1, \ldots, n-1\}$ possible remainders mod n.

In $\mathbb{Z}/_n$ $n \equiv 0$ so we add and multiply in the usual way but when we see n we write 0.

(eg) $\mathbb{Z}/_3 = \{0, 1, 2\}$

+	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

$\mathbb{Z}/_3$ is a field because every non zero element has a mult inverse, so we write it as $\mathbb{F}_3$

(eg)

$\mathbb{Z}/4 = \{0,1,2,3\}$

+	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

$\mathbb{Z}/4$ is not a field because $2 \neq 0$ but ther is no mult inverse for 2 (no 1s) So $\mathbb{Z}/4$ is <u>not</u> written $\mathbb{F}_4$.

We'll see that $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime. So when p is prime we write $\mathbb{F}_p$ rather than $\mathbb{Z}/p$

(eg) Take field $\mathbb{F}$. $\mathbb{F}(x) = \{$polys in x with coeffs in $\mathbb{F}\}$

$a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ $\quad (a_i \in \mathbb{F})$

So we can add, multiply in $\mathbb{F}(x)$ as you do at school.

General Construction:

$\mathbb{F}$ field. Let $a(x) = a_n x^n + a_{n-1}a^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}(x)$

where $a_n \neq 0$ $\quad \boxed{\deg a = n}$

$\mathbb{F}(x)/a(x)$ Add and multiply as usual but every time we see $a(x)$ we write $a(x) \equiv 0$.

(eg) $\mathbb{F}_4$, the field with 4 elements. Start with $\mathbb{F}_2 = \{0,1\}$ $\quad 1+1=0$

Next take $\mathbb{F}_2(x)$ = polynomials in x over $\mathbb{F}_2$

Take $a(x) = x^2+x+1$

Represent $\mathbb{F}_2(x)/x^2+x+1$ as the possible remainders I can get when I divide by x^2+x+1 ~ deg 2.

Possible remainders have deg ≤ 1

So possible remainders are $0, 1, x, x+1$ (All polys of degree ≤ 1)

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

$\cdot$	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

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

x^2+x? $x^2+x\equiv -1\equiv 1$

$x^2+\cancel{2x}+1$ $x^2+1\equiv -x\equiv x$

so $\mathbb{F}_4 = {}^{\mathbb{F}_2(x)}/_{x^2+x+1}$

First historical example : ${}^{\mathbb{Q}(x)}/_{x^2-2}$ x^2-2 has no factorisation over $\mathbb{Q}$

${}^{\mathbb{Q}(x)}/_{x^2-2}$ is a field. Elements are $a+bx$ $a,b\in\mathbb{Q}$

$x^2-2\equiv 0$ $x^2\equiv 2$ Usually write $x=\sqrt{2}$

Algebra <u>Sheet 5</u> (PC) 28th Feb

$|G| = 55 = 5 \cdot 11$

$N_{11} \equiv 1 (\bmod 11)$ If $N_{11} = 1$ then $N_{11} \geq 12$

Let k be a subgroup of order 11. $K \cong C_{11}$

If $N_{11} \geq 12$ $K = K_1, K_2, \dots, K_{12}$ got at least $\overset{=120}{12 \times (11-1)}$ elements of order 11. But $|G| = 55$ so $N_{11} = 1$ and K is the unique of order 11 $K \trianglelefteq G$.

Let Q be a subgroup of order 5. $K \cap Q = \{1\}$ $|K||Q| = |G|$

Apply recog $G \cong C_{11} \rtimes_h C_5$ $h : C_5 \to \mathrm{Aut}(C_{11})$

$$\begin{array}{cccccccccccc}\mathrm{Aut}(C_{11}) = \{ & \varphi_1, & \varphi_2, & \varphi_4, & \varphi_8, & \varphi_5, & \varphi_{10}, & \varphi_9, & \varphi_7, & \varphi_3, & \varphi_6 & \} \cong C_{10} \\ & \mathrm{Id} & \alpha & \enclose{circle}{\alpha^2} & \alpha^3 & \enclose{circle}{\alpha^4} & \alpha^5 & \enclose{circle}{\alpha^6} & \alpha^7 & \enclose{circle}{\alpha^8} & \alpha^9 & \end{array}$$

$C_5 \to \mathrm{Aut}(C_{11})$ must ~~have~~ hit elements of order 5 or <u>1</u>

$h_0 : C_5 \to \mathrm{Aut}(C_{11})$ $C_5 = \{1, y, \dots, y^4\}$

$h_0(y) = \mathrm{Id} \rightsquigarrow \underline{C_{11} \times C_5} \cong C_{55}$

$h_1(y) = \alpha^2$ $YXY^{-1} = X^4$

$h_2(y) = \alpha^4$ $YXY^{-1} = X^5$

$h_3(y) = \alpha^6$ $YXY^{-1} = X^9$

$h_4(y) = \alpha^8$ $YXY^{-1} = X^3$

All isomorphism:

$Y^2XY^{-2} = YX^4Y^{-1} = (YXY^{-1})^4 = X^{16} = X^5$

$Y^3XY^{-3} = X^9$

$Y^4XY^{-4} = X^3$

So only 2 groups of order 55, $C_{11} \times C_5 \cong C_{55} = \langle X, Y \mid X^{11} = Y^5 = 1 \quad YX = XY \rangle$

$G(55) = \langle X, Y \mid X^{11} = Y^5 = 1, YXY^{-1} = X^4 \rangle$

③ $|G| = 12 = 4 \cdot 3 = 2^2 \cdot 3$

Still go for larger prime : $p=3$ $q=2$.

$\exists$ subgroup H : $|H| = 3$

L : $|L| = 4$

$N_3 \equiv 1 \pmod{3}$ $N_3 = 1$ or 4 or $N_7 \geq 7$

$N_7 \geq 7$ gives at least 14 elements of order 3 ⨳

Suppose $N_3 = 4$. Then $\exists$ exactly $4 \times (3-1) = 8$ elements of order 3.

Still $12 - 8 = 4$ elements unaccounted for, and L is a subgroup of order 4 so L accounts for missing elements when $N_3 = 4$.

ie if $N_3 = 4$ then $N_2 = 1$.

So either $N_3 = 1$ and $H \lhd G$ or $N_3 = 4$ and $N_2 = 1$ and $L \lhd G$

So now get either

i) $C_3 \rtimes C_4$ } when $H \lhd G$ L either C_4 or $C_2 + C_2$

ii) $C_3 \rtimes C_2 \times C_2$ }

or

iii) $C_4 \rtimes C_3$ } when $L \lhd G$ $L \cong C_4$ or $C_2 + C_2$

iv) $(C_2 \times C_2) \rtimes C_3$ }

Algebra Sheet 6 (PC) 2nd March '12

③ $|G|=8$ $\boxed{\exists y \in G \text{ st } \mathrm{ord}(y)=4}$

Take $H=\{1,y,y^2,y^3\}$ Take $x \in G-H$

i) Show $x^2 \in H$. Firstly, $xH \neq H$ (otherwise $x \in H$ which isn't true)

$\left|G/H\right| = 2$ so only two cosets $G = H \sqcup xH$

look at x^2H. A priori x^2H = either H or xH.

If $x^2H = xH$ then $x^{-1}x^2H = H$ so $xH = H$ ✗.

so $x^2H = H$. By rule of equality $x^2 1^{-1} \in H$ ie $x^2 \in H$ □.

So apriori $P_1 : x^2 = 1$

$P_2 : x^2 = y$

$P_3 : x^2 = y^2$

$P_4 : x^2 = y^3$

H has index 2 in G so $H \trianglelefteq G$ so we know $xyx^{-1} \in H$

But $\mathrm{ord}(xyx^{-1}) = \mathrm{ord}(y)$ because conjugation by x is an ~~iso~~automorphism so preserves order.

$$(xyx^{-1})^2 = xyx^{-1}xyx^{-1} = xy^2x^{-1}$$

$$(xyx^{-1})^3 = xy^2x^{-1}xyx^{-1} = xy^3x^{-1}$$

$$(xyx^{-1})^4 = xy^3x^{-1}xyx^{-1} = x1x^{-1} = 1$$

$\mathrm{ord}(1)=1$ $\mathrm{ord}(y)=4$ $\mathrm{ord}(y^2)=2$ $\mathrm{ord}(y^3)=4$

$\mathrm{ord}(xyx^{-1})=4$ so either

$Q1 : xyx^{-1} = y$ $Q2 : xyx^{-1} = y^3$

(P1,Q1) $x^2=1$ $xyx^{-1}=y$ $\rightarrow C_2 \times C_4$ x, y

P1,Q2) $x^2=1$ $xyx^{-1}=y^3$ $\longrightarrow D_8$ $\langle y, x \mid y^4=x^2=1 \; xyx^{-1}=y^3 \rangle$

2,Q1) $x^2=y$ $xyx^{-1}=y$ $\rightarrow C_8$ $\text{ord}(x)=8$ $y=x^2$

2,Q2) $x^2=y$ $xyx^{-1}=y^3$ $\rightarrow$ subtle. $\text{Ord}(x)=8$ $y=x^2$ But $xy \neq yx$ so
NO SUCH GROUP. $x(x^2) \neq (x^2)x$ ✗

3,Q1) $x^2=y^2$ $xyx^{-1}=y$ $\rightarrow C_2 \times C_4$. Put $z=xy$, $z^2=xyxy=xxyy=x^2y^2$
$=y^4=1$

3,Q2) $x^2=y^2$ $xyx^{-1}=y^3 \rightarrow Q_8$ $x=i$ $y=j$ $x^2=y^2=-1$
$ij(-i)=-iji=+i^2j=-j$ $xyx^{-1}=y^3$

4,Q1) $x^2=y^3$ $xyx^{-1}=y$ $\longrightarrow C_8$ $\text{ord}(x)=8$ $\text{ord}(y^3)=4$ $y=x^6$

4,Q2) $x^2=y^3$ $xyx^{-1}=y^3 \rightarrow$ $\text{ord}(x)=8$, should be C_8 but x doesn't commute
with one of its powers ✗ - NO SUCH GROUP.

So if G has order 8 and $\exists y \in G$ $\text{ord}(y)=4$ then
$G \cong C_8, C_2 \times C_4, D_8$ or Q_8

Remaining possibility $\forall g \in G$ $g^2=1$. $G \cong C_2 \times C_2 \times C_2$

So there are exactly 5 groups of order 8.

Algebra 4 2nd March '12

GROUPS of ORDER 12

I) $G \cong C_3 \rtimes C_4$ $\qquad$ Q_8 not a semidirect product.

II) $G \cong C_3 \rtimes (C_2 \times C_2)$

III) $G \cong C_4 \rtimes C_3$

IV) $G \cong (C_2 \times C_2) \rtimes C_3$

(I) $C_3 = \{1, x, x^2 / x^3 = 1\}$ $\qquad$ $C_4 = \{1, y, y^2, y^3\}$

$YXY^{-1} = X$: Trivial homo $C_4 \to Aut(C_3)$ $\qquad$ $C_3 \times C_4$

or $YXY^{-1} = X^2$: $Y^4 = 1$ $\qquad$ $D_6^* = \langle X, Y \mid X^3 = Y^4 = 1 \quad YXY^{-1} = X^2 \rangle$

(II) There are 4 homos. $C_2 \times C_2 \to Aut(C_3) = \{1, \tau\}$ $\quad$ $\tau(x) = x$

$h_0(s) = h_0(t) = h_0(st) = 1$ $\qquad$: $C_3 \times C_2 \times C_2$

$$\left.\begin{array}{lll} h_1(s) = \tau & h_1(t) = 1 & h(st) = \tau \\ h_2(s) = 1 & h_2(t) = \tau & h(st) = \tau \\ h_3(s) = \tau & h_2(t) = \tau & h(st) = 1 \end{array}\right\} \quad D_6 \times C_2 \begin{array}{l} h_1 : \langle x, s\rangle, \langle t \\ h_2 : \langle x, t\rangle, \langle s \\ h_3 : \langle x, s\rangle, \langle st \end{array}$$

generators ↑

(III) $C_3 \to Aut(C_4) = C_2$ necessarily trivial

$C_4 \times C_3 \cong C_{12}$

(IV) $C_2 \times C_2 \times C_3$ or A_4 (twice)

So exactly 5 groups of order 12.

$C_{12} = C_4 \times C_3$, $\quad C_6 \times C_2$, $\quad D_6 \times C_2$, $\quad D_6^*$, $\quad A_4$

Ideals and Quotient Rings

Let R be a (commutative) ring. By an ideal I in R we mean that i) I is an additive subgroup of R, such that

ii) $\forall x \in I \; . \; \forall \lambda \in R \quad \lambda x \in I$ (technically a LEFT Ideal)

If I is an ideal in R we write $\boxed{I \lhd R}$

ⓔⓖ Let $R = \mathbb{Z}$.

$I = \{\text{even integers}\} = \{2n : n \in \mathbb{Z}\}$

So I is an additive subgroup $\left\{\begin{array}{l} 2n+2m = 2(n+m) \\ 0 = 2 \cdot 0 \\ 2n+2(-n) = 0 \end{array}\right\}$

Also if $\lambda \in \mathbb{Z}$ $2n \in I$, $\lambda 2n = 2(\lambda n) \in I$ so I is an ideal in $\mathbb{Z}$

Generalisation: Take $n \in \mathbb{Z}$ and take $I = (n) \underset{\text{defn.}}{=} \{\lambda n : \lambda \in \mathbb{Z}\}$

Then $(n) \lhd \mathbb{Z}$

Even greater generalisation

Let R be a commutative ring. Let $\alpha \in R$. Define $\cancel{(\alpha)}$

$(\alpha) = \{\lambda \alpha : \lambda \in R\}$ Then (α) is an ideal in R.

Quotient Ring Construction

Let R be a commutative ring, and $I \lhd R$ an ideal. Because I is an additive subgroup, Form R/I quotient group.

elements of R/I have form $\boxed{x + I, \; x \in R}$

RULE OF EQUALITY (for additive cosets)

$\boxed{x + I = x' + I \iff x - x' \in I}$

R/I is obviously an abelian group.

$\boxed{(x+I) + (y+I) = (x+y) + I}$ Zero element is $0 + I = I$

Inverses: $(-x) + I = -(x+I)$

Proposition: Let R be a commutative ring, and $I \lhd R$ an ideal. Then R/I has a natural ring structure.

Proof: Addition on R/I given above. Need to define result

$$\boxed{\cdot : R/I \times R/I \longrightarrow R/I} \quad \boxed{(x+I)\cdot(y+I) \overset{\text{defn}}{=} xy+I}$$

Must show that $\cdot$ is well defined, ie Suppose

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

got to show that $\boxed{xy+I = x'y'+I}$.

ie $(x-x' \in I) \wedge (y-y' \in I) \implies xy - x'y' \in I$.

Standard Trick:

$$xy - x'y' = xy - xy' + xy' - x'y' = x(y-y') + (x-x')y'$$

(R commutative) so $x(y-y') = y'(x-x')$

$$\left.\begin{array}{l} y-y' \in I \text{ so } x(y-y') \in I \\ x-x' \in I \text{ so } y'(x-x') \in I \end{array}\right\} \implies xy - x'y' \in I$$

I additive subgroup.

So $\cdot$ is well defined.

Need to check that $R/I = (R/I, +, \underset{\substack{\uparrow\\0+I}}{0}, \cdot, \underset{\substack{\uparrow\\1+I}}{1})$ is a ring

Multiplicative Identity is $1+I$

$(x+I)(1+I) = x\cdot 1 + I = x+I$

Multiplication is associative

$(x+I)\cdot[(y+I)\cdot(z+I)] = (a+I)(yz+I) = x(yz)+I = (xy)z+I$

$= (xy+I)(z+I) = [(x+I)(y+I)](z+I)$ you do the rest.

(eg) $R = \mathbb{Z}$ $I = (2) = \{\text{even integers}\}$

$\mathbb{Z}/(2)$ has exactly two elements.

Two cosets are $\underset{\substack{\shortparallel\\0+(2)}}{(2)}$ and $\underset{\substack{\shortparallel\\\{\text{odd integers}}}{1+(2)}$

Multiplication on $\mathbb{Z}/(2)$

$\cdot$	$0+(2)$	$1+(2)$
$+(2)$	$0+(2)$	$0+(2)$
(2)	$0+(2)$	$1+(2)$

$+$	$0+(2)$	$1+(2)$
$0+(2)$	$0+(2)$	$1+(2)$
$1+(2)$	$1+(2)$	$0+(2)$

$\mathbb{Z}/2$ is simply $\mathbb{F}_2$ the field with two elements.

(eg) $R=\mathbb{Z}$ $I=(3)$ $\mathbb{Z}/(3)$ has 3 elements $0+(3)$, $1+(3)$, $2+(3)$

Prop: $R=\mathbb{Z}$ $I=(n)$ $n>0$
Then $\mathbb{Z}/(n)$ has exactly n elements

$0+(n), 1+(n), \ldots, n-1+(n)$ ← bracket is "ideal"

If $N \geq n$ divide $N = qn + r$ $N+(n) = r+(n)$, $qn \in (n)$
$0 \leq r \leq n-1$

and $\mathbb{Z}/(n)$ is what we have called $\mathbb{Z}/n$. We'll show $\mathbb{Z}/n$ is a field $\Leftrightarrow$ n is prime. We need an intermediate concept.

Defn: Say that a (commutative) ring R is an INTEGRAL DOMAIN when if $a,b \in R$ and $ab=0$ then either $a=0$ or $b=0$

egs) 1: $\mathbb{Z}$ is an integral domain.
2: Any field is an integral domain. (but not every integral domain is a field)

3: $\mathbb{Z}/4$ is not an integral domain
Write $[x] = x+(4)$ $[2][2]=0$ but $[2] \neq [0]$

Prop: A finite ~~(commutative~~ integral domain, A, is a field (Assume commutative but not necessary)

Proof: A finite commutative ring satisfying "$ab=0 \Rightarrow a=0$ or $b=0$".
Let $a \in A$, $a \neq 0$. Need to find $y \in A$: $ay=1$
Consider $\lambda: A \to A$, $\lambda(x)=ax$. λ is a homo of additive groups
$\lambda(x+y) = a(x+y) = ax+ay = \lambda(x)+\lambda(y)$
λ is injective. Suppose $\lambda(x_1)=\lambda(x_2)$ then $ax_1 = ax_2$ so $a(x_1-x_2)=0$
because $a \neq 0$ must have $x_1-x_2=0$, $x_1=x_2$. An injective map $\lambda: \binom{\text{finite}}{\text{set } A} \to \binom{\text{finite}}{\text{set } A}$ has to be surjective. So λ is surj. So $\exists y \in A$ $\lambda(y)=1$ ie $\exists y \in A$ $ay=1$ $\square$.

Algebra 4 8   6th March 2012

$\mathbb{Z}/_n$ is obviously finite $n \geq 2$. Then we have n distinct elements

$[0], [1], \ldots, [n-1] \quad ([r] = \{r + n\mathbb{Z}\})$

Prop: $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime.

Proof ($\Rightarrow$) show the contrapositive ie n is not a prime $\Rightarrow$ $\mathbb{Z}/_n$ not an integral domain. Suppose n not a prime $n = pk$, p prime, $k \geq 2$

Then $[p][k] = [n] = 0$ in $\mathbb{Z}/_n$ But $[p] \neq 0$ $[k] \neq 0$

$p < n$ $k < n$ so $\mathbb{Z}/_n$ not integral domain. $\boxed{\Rightarrow}$

($\Leftarrow$) Suppose n is prime. Suppose $[r], [s] \in \mathbb{Z}/_n$. Satisfy $[r][s] = 0 \in$

ie $rs = \alpha n$ for some $\alpha \in \mathbb{Z}$

Because n is prime, get either

n divides r so $[r] = 0$

or n divides s so $[s] = 0$ So n is prime and

$[r][s] = 0 \Rightarrow [r] = 0$ or $[s] = 0$ ie $\mathbb{Z}/_n$ integral domain $\boxed{\Leftarrow}$

Corollary: $\mathbb{Z}/_n$ is a field $\Leftrightarrow$ n is prime.

Pf: $\mathbb{Z}/_n$ is a finite ring. So $\mathbb{Z}/_n$ is a field $\Leftrightarrow$ $\mathbb{Z}/_n$ integral domain.

$\Leftrightarrow$ n prime $\square$.

We now give a parallel case

Two typical rings:

$\mathbb{Z} \hookrightarrow \{\mathbb{F}[x]$ ring of polys in x with coeffs in field $\mathbb{F}\}$

Very similar properties

Instead of $\mathbb{Z}/_n$ we'll look at $\mathbb{F}[x]/_{p(x)}$ where $p(x)$ is some nonzero polynomial.

Question: How should we represent (practically) the elements of $\mathbb{F}[x]/_{p(x)}$

Analogy: In $\mathbb{Z}/_n$: $[N] = [r]$ when $N = qn + r$

ie divide N by n and take remainder.

In $\mathbb{F}[x]/p(x)$ $\quad [a(x)] = [\gamma(x)]$ where $a(x) = q(x)p(x) + r(x)$

ie divide $a(x)$ by $p(x)$ and take remainder.

Division Algorithm for Polynomials

Work in $\mathbb{F}(x)$. $\mathbb{F}$ field. If $p(x)$ has degree n and $a(x)$ has degree $N \geq n$ can divide $a(x)$ by $p(x)$ to get $a(x) = q(x)p(x) + r(x)$ and $\boxed{\deg(r) < \deg(p) = n}$

and note

$$a(x) - r(x) = q(x)p(x) \in \overset{\text{Ideal}}{[p(x)]}$$

So if I write $\begin{cases} [a(x)] \text{ for } a(x) + [p(x)] \\ [\gamma(x)] \text{ for } r(x) + [p(x)] \end{cases}$ then $[a(x)] = [\gamma(x)]$

So we represent elements of $\left(\mathbb{F}[x]/p(x)\right)$ by the possible remainders $r(x)$ $\quad \deg r(x) < \deg p(x) = n$

Representation Convention: We represent elements of $\mathbb{F}[x]/p(x)$ by polynomials $r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \dots + r_1 x + r_0$

$$r_0 \dots r_{n-1} \in \mathbb{F}$$

Observe that

Prop: $\mathbb{F}[x]/p(x)$ is a vector space over $\mathbb{F}$ and $\dim_{\mathbb{F}}\left[\frac{\mathbb{F}[x]}{p(x)}\right] = \deg(p(x))$

[simple eg: $p(x) = x^3 + x^2 + 2x + 1$

Possible remainders ($\deg p = 3$) $\quad r_2x^2 + r_1x + r_0 \quad \dim \frac{\mathbb{F}[x]}{p(x)} = 3$]

Pf: Have a basis

$1, x, \dots, x^{n-1}$ with n elements $\square$.

Theorem: Let A be a ring such that (commutative)

i) A contains a field $\mathbb{F}$ as a subring

ii) $\dim_{\mathbb{F}}(A)$ is finite (finite dimensional)

Then A is an integral domain $\Leftrightarrow$ A is a field.

Proof ($\Leftarrow$) Trivial

($\Rightarrow$) Suppose A integral domain, let $a \in A$ $a \neq 0$. I have to find $b \in A$ s.t. $ab = 1$. Consider $\lambda_a : A \to A$

$\lambda_a(y) = ay$.

λ_a is linear. $\lambda_a(y_1 + y_2) = a(y_1 + y_2) = ay_1 + ay_2 = \lambda_a(y_1) + \lambda_a(y_2$

$\lambda_a(\xi y) = a(\xi y) = (a\xi)y = (\xi a)y = \xi(ay) = \xi \lambda_a(y) \Rightarrow \lambda_a$ linear

As $\dim A$ finite apply Kernel-Rank Thm

$\dim \operatorname{Ker}(\lambda_a) + \dim(\operatorname{Im} \lambda_a) = \dim A$

But $\operatorname{Ker} \lambda_a = 0$ why?

$\lambda_a(y) = 0 \Rightarrow ay = 0$ and $a \neq 0$

so $y = 0$ (A integral domain)

So $\dim \operatorname{Im} \lambda_a = \dim A$ so λ_a surjective.

So $\exists b \in A$ $\lambda_a(b) = 1$

$\exists b \in A$ $ab = 1$ and A is a field $\square$.

Beware Result is definietely false if $\dim A = +\infty$.

(eg) $A = \mathbb{F}[x]$. A is ∞ dim · has bases $1, x, x^2, \ldots, x^n, x^{n+1}, \ldots$

$\mathbb{F}[x]$ is an integral domain but $\mathbb{F}[x]$ is not a field.

x has no inverse.

$\mathbb{F}[x]/p(x)$ is finite dimensional $/\mathbb{F}$

Obvious Question: What is $\mathbb{F}[x]/p(x)$ an integral domain?

Recall

Defn: $p(x) \in \mathbb{F}[x]$, $p(x) \neq 0$ is said to be irreducible over $\mathbb{F}$ when $p(x) = a(x)b(x)$ $\Rightarrow a(x)$ is a constant or $b(x)$ is a constant

Equivalently, $p(x)$ irred $/\mathbb{F}$ when $p(x) = a(x)\,b(x)$ $\Rightarrow \deg a(x) = 1$ and $\deg b(x) = \deg p(x)$ or $\deg(a(x)) = \deg p(x)$ and $\deg b(x) = 1$

So well prove

<u>hm</u>: $\deg p(x) \geq 1$ $p(x) \in \mathbb{F}[x]$. Then $\mathbb{F}[x]/p(x)$ is an integral domain $\iff$ $p(x)$ irred $/\mathbb{F}$.

In $\mathbb{F}[x]$ every poly of $\deg \geq 2$ can be expressed uniquely
$p(x) = C a_1(x) \ldots a_m(x)$ where $C \in \mathbb{F}$
and $a_1(x)$ $a_m(x)$ irreducible and <u>monic</u>. (leading coeff $= 1$)
(Unique up to order)

<u>hm</u>: $p(x) \in \mathbb{F}[x]$ $\deg p(x) \geq 1$

$\frac{\mathbb{F}[x]}{p(x)}$ is an integral domain $\iff$ $p(x)$ is irreducible over $\mathbb{F}$.

<u>Pf</u>: $(\Rightarrow)$ Easier to look at contrapositive.
ie if $p(x)$ is not irreducible $\Rightarrow$ $\mathbb{F}[x]/p(x)$ is not an integral domain.
If $p(x)$ is not irreducible then write $p(x) = a(x)b(x)$
$1 \leq \deg a < \deg p$ and $1 \leq \deg b < \deg p$
so now $[a(x)][b(x)] = [p(x)] = 0$ on $\mathbb{F}[x]/p(x)$
but $[a(x)] \neq 0$ and $[b(x)] \neq 0$ $\boxed{\Rightarrow}$

$(\Leftarrow)$ Suppose $p(x)$ is irreducible and suppose $a(x), b(x) \in \mathbb{F}[x]$
such that $[a(x)][b(x)] = 0$ on $\mathbb{F}[x]/p(x)$
ie $a(x)b(x) = q(x)\,p(x)$ for some $q(x)$
Decompose $a(x), b(x)$ into products of irreducibles.
$a(x) = A\alpha_1(x) \ldots \alpha_m(x)$ $b(x) = B\beta_1(x) \ldots \beta_n(x)$ $\|$ $a_i(x)$, $b_j(x)$ irreducible.

$a(x)\,b(x) = AB\,\alpha_1(x) \ldots \alpha_m(x)\beta_1(x) \ldots \beta_n(x) = q(x)p(x)$
By uniqueness of factorisation because $p(x)$ is irreducible on RHS it must also be on LHS. So either $\alpha_i(x) = (\text{constant})\,p(x)$ for some i (I)
or $\beta_j(x) = (\text{constant})\,p(x)$ for some j (II)

If (I) then $p(x)$ divides $a(x)$ and $[a(x)] = 0$

If (II) then $p(x)$ divides $b(x)$ and $[b(x)] = 0$

Either way, $[a(x)][b(x)] = 0 \Rightarrow [a(x)] = 0$ or $[b(x)] = 0$ $\square$

Corollary: Let $\deg p(x) \geq 1$ $p(x) \in \mathbb{F}[x]$ $\mathbb{F}$ field.
Then following conditions are equivalent.

i) $\mathbb{F}[x]/p(x)$ is a field

ii) " " an integral domain

iii) $p(x)$ irreducible.

So this is a way of constructing new fields from old fields.
$\mathbb{F}$ field I have seen before.

$p(x)$ irreducible polynomial in $\mathbb{F}[x]$. $\mathbb{F}[x]/p(x)$ is then a new field

(egs) 1) $\mathbb{F} = \mathbb{C}$ (Boring)

Let $p(x) \in \mathbb{C}[x]$. $\deg p(x) \geq 1$. When is $p(x)$ irreducible?
Only when $p(x) = A(x-\lambda)$ linear. Every poly in $\mathbb{C}[x]$ is a product of linear factors.

$\mathbb{C}[x]/x-\lambda \cong \mathbb{C}$ $\quad \dim_{\mathbb{C}}\left(\mathbb{C}[x]/x-\lambda\right) = 1$ and $\mathbb{C} \subset \mathbb{C}[x]/x-\lambda$

so $\mathbb{C}[x]/x-\lambda \cong \mathbb{C}$ Gives nothing new

2) Slightly more interesting. $\mathbb{F} = \mathbb{R}$.

$p(x) \in \mathbb{R}[x]$ $\deg p(x) \geq 1$. When is $p(x)$ irreducible over $\mathbb{R}$?

Irred polys over $\mathbb{R}$: one of two sorts.

i) $p(x) = A(x-\lambda)$ linear, $A, \lambda \in \mathbb{R}$

ii) $p(x) = ax^2 + bx + c$ $\quad b^2 - 4ac < 0$

$\mathbb{R}[x]/_{x-\lambda} \cong \mathbb{R}$ $\qquad$ $\dfrac{\mathbb{R}[x]}{ax^2+bx+c} \cong \mathbb{C}$ $\qquad$ $(b^2-4ac<0)$

3) Much more interesting $\mathbb{F}=\mathbb{Q}$ cont...

somorphism of Rings

Let R, S be rings. By a ring homomorphism $\varphi: R \to S$ I mean a mapping such that

i) $\varphi(x+y) = \varphi(x) + \varphi(y)$

ii) $\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in R.$

iii) $\varphi(1_R) = 1_S$

By a ring isomorphism $\varphi: R \cong S$ I mean a bijective homo

Defn: Let R_1, R_2 be rings. By $\boxed{R_1 \times R_2}$ we mean the ring obtained thus:

$$(x_1, x_2) + (y_1, y_2) = (x_1+y_1, x_2+y_2)$$

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$$

$$1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$$

$$1 = (1,1)$$

hint 3d) sheet 8

In $R_1 \times R_2$ you get elements $e_1 = (1,0)$ $\quad e_2 = (0,1)$ $\quad \left\{ 1 = e_1 + e_2 \right.$

$\left. e_1^2 = e_1 \quad e_2^2 = e_2 \quad e_1e_2 = e_2e_1 \right\} \iff \boxed{\text{Idempotents}}$

t ought to be clear that we get more types of irreducible $/\mathbb{Q}$ than over $\mathbb{R}$.

eg) $\sqrt{2} \notin \mathbb{C}$. Over $\mathbb{R}$ can factorise $(x^2-2) = (x-\sqrt{2})(x+\sqrt{2})$ but it is not a factorisation over $\mathbb{Q}$: x^2-2 irred $/\mathbb{Q}$

$\mathbb{Q}[x]/_{x^2-2} = \{a+bx : a,b \in \mathbb{Q} \quad x^2-2=0 \quad x^2=2\}$

So we can think of x as $\sqrt{2}$ $\quad \mathbb{Q}[x]/_{x^2-2} = \{a+b\sqrt{2} \quad a,b \in \mathbb{Q}\}$

Kronecker c. 1860 AD.

Eisenstein's Criterion (c 1850)

Let p be prime.

$a(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

where $a_n, \dots, a_0 \in \mathbb{Z}$ st

i) $a_n \not\equiv 0 \pmod p$

ii) $a_r \equiv 0 \pmod p$ $\quad 0 \le r \le n-1$

iii) $a_0 \not\equiv 0 \pmod{p^2}$

Then $a(x)$ is irred over $\mathbb{Q}$

Ⓔⓖ $p=7$. $\quad x^{100} + 49x^{51} + 14x^2 + \underset{3 \cdot 7}{\underset{\shortparallel}{21}}$ irred over $\mathbb{Q}$

Algebra 4 9th March 2012

Eisensteins Criterion

Let p be a prime. $a(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ (Integer polynomial) such that

i) $a_n \not\equiv 0 \pmod{p}$

ii) $a_r \equiv 0 \pmod{p}$ $\quad 0 \le r \le n-1$

iii) $a_0 \not\equiv 0 \pmod{p^2}$

Then $a(x)$ is irreducible over $\mathbb{Q}$

(eg) $x^{100} + 43x^{57} + 86$

Irreducible ~~over~~ $\mathbb{Q}$ $\quad p = 43$

(eg) $y^4 + 4y^3 + 6y^2 + 4y + 4 = a(y)$

with $p = 2$ this fails on the constant

$4 \equiv 0 \pmod{2^2}$

(eg) $a(y) = (y+1)^4 + 3$

if I put $x = y+1$ $\quad x^4 + 3$

which passes Eisensteins with $p = 3$

if $a(y) = a_1(y)a_2(y)$ $\quad \deg a_i < 4$

i'd get a factorisation

$x^4 + 3 = a_1(x-1)a_2(x-1)$

But there is no such factorisation because x^4+3 is irred.

So can substitute $y = x + a$ $\quad a \in \mathbb{Z}$ and try again.

(eg) Let p be a prime.

Define $C_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$

So $\boxed{x^p - 1 = (x-1)C_p(x)}$ Cyclotomic polynomial

Prop: $C_p(x)$ is irreducible over $\mathbb{Q}$

Proof: $x^p - 1 = (x-1)C_p(x)$

$\left(\frac{x^p-1}{x-1}\right) = C_p(x)$ Put $y = x-1$ or $x = y+1$

$$x^p = (y+1)^p = y^p + \sum_{r=1}^{p-1}\binom{p}{r}y^r + 1$$

So $x^p - 1 = y^p + \sum_{r=1}^{p-1}\binom{p}{r}y^r$

$$C_p(x) = \left(\frac{x^p-1}{x-1}\right) = \frac{y^p + \sum_{r=1}^{p-1}\binom{p}{r}y^r}{y} = y^{p-1} + \sum_{r=1}^{p-1}\binom{p}{r}y^{r-1}$$

$\begin{bmatrix}\text{Put } s = r-1 \\ r = s+1\end{bmatrix}$ $= y^{p-1} + \sum_{s=0}^{p-2}\binom{p}{s+1}y^s = y^{p-1} + \sum_{s=1}^{p-2}\binom{p}{s+1}y^s + p$ □.

This satisfies Eisensteins so $C_p(x)$ is irred$/\mathbb{Q}$

Defn: Say that a polynomial $a(x) \in \mathbb{Z}[x]$, $\deg(a) = n \geq 2$ has <u>no proper factorisation over $\mathbb{Z}$</u> when there is no factorisation $a(x) = b(x)c(x)$ where $b(x), c(x) \in \mathbb{Z}[x]$ and $\deg b(x) < n$, $\deg c(x) < n$

(not just irreducibility)

Thm: (Eisenstein over $\mathbb{Z}$)

Let p be a prime. Let $a(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

where $a_0 \dots a_n \in \mathbb{Z}$ s.t.

i) $a_n \not\equiv 0 \bmod p$

ii) $a_r \equiv 0 \bmod p$ $\quad 0 \leq r \leq n-1$ $\quad \Longrightarrow$ Then $a(x)$ has no proper factorisation over $\mathbb{Z}$.

iii) $a_0 \not\equiv 0 \bmod p^2$

Proof : Suppose you can write $a(x) = b(x)c(x)$

$$\left.\begin{array}{l} b(x) = b_k x^k + \dots + b_1 x + b_0 \\ c(x) = c_l x^l + \dots \; c_1 x + c_0 \end{array}\right\} \begin{array}{l} b_k \neq 0 \\ c_l \neq 0 \end{array}$$

~~So that~~ with $k < n$, $l < n$ and $k + l = n$.

$a(x) = a_n x^n + \dots + a_1 x + a_0$

Look at constant terms

$a_0 = b_0 c_0$

a_0 is divisible by p, but not by p^2 So either wlog assume

$p \mid b_0$ and $p \nmid c_0$ OR $p \nmid b_0$ and $p \mid c_0$

Next look at coeffs of x.

$$\boxed{a_1 = b_0 c_1 + b_1 c_0}$$

$a_1 \equiv 0 \bmod p$ so LHS divisible by p so RHS is divisible by p. c_0 is divisible by p so $b_0 c_1$ is divisible by p. $p \nmid b_0$ so c_1 is divisible by p.

s not 5

We'll show by induction on s that each c_s is divisible by p.

True already for $s = 0, 1$. Suppose proved $\boxed{\text{for } < s}$ and consider coeffs of x^s $\boxed{s < n}$

$$a_s = b_0 c_s + b_1 c_{s-1} + \dots + b_s c_0$$

$$a_s = b_0 c_s + \sum_{t=1}^{s} b_t c_{s-t}$$

By hypothesis $a_s \equiv 0 \bmod p$ so RHS is divisible by p.

By Induction hypothesis each c_{s-t} is divisible by p $(1 \leq t \leq s)$

So $b_0 c_s$ is divisible by p. But $p \nmid b_0$ so $p \mid c_s$

So by induction $c_s \equiv 0 \bmod p$ for $0 \leq s < l$

Now look at coeffs of x^n $a_n = b_k c_l$

Shown $c_\ell \equiv 0 \mod p$ Hence $\times$
$a_n \equiv 0 \mod p$

Hence no such factorisation exists $\Box$.

<u>Coeffs of x^2</u>

divisible by p

$$a_2 = \boxed{b_0 c_2} + \cancel{b_1 c_1} + \cancel{b_2 c_0}$$

induction shown its div by p

must be div by p.

iv by p

Still need to show "Gauss' Lemma"

If $a(x) \in \mathbb{Z}[x]$ has no proper factorisation over $\mathbb{Z}$ then $a(x)$ also has proper factorisation over $\mathbb{Q}$

Algebra 4 13th March 2012

If $a(x) \in \mathbb{Z}[x]$ has no proper factorisation of $\mathbb{Z}$ then $a(x)$ has no proper factorisation over $\mathbb{Q}$.

Defn: Let $a(x) = a_n x^n + .. + a_0$, $a_r \in \mathbb{Z} \ \forall r$

Define the content $C(a)$ to be $HCF(a_n, a_{n-1}, .., a_0)$

Can factorise $a(x) = C(a)\, a_0(x)$ where $a_0(x) \in \mathbb{Z}[x]$, $C(a_0) = 1$

Gauss' Lemma

$$[C(b) = 1] \wedge [C(c) = 1] \Rightarrow C[b(x)c(x)] = 1$$

Proof: Write $a(x) = b(x)c(x)$ $b(x) = b_m x^m + .. + b_0$

$c(x) = c_n x^n + .. + c_0$

Suppose $C(b) = 1$, $C(c) = 1$ but $C(a) \neq 1$

Then for at least one prime p , p divides each a_r :

$a(x) = a_{m+n} x^{m+n} + .. + a_0$

Put $k = \min\{r : p \nmid b_r\}$ $l = \min\{r : p \nmid c_r\}$

Then p divides b_r when $r < k$. p divides c_r when $r < l$

Consider $a_{k+l} = b_k c_l + \sum_{r>1} b_{k-r} c_{l+r} + \sum_{r \geq 1} b_{k+r} c_{l-r}$

NB: $\sum_{r \neq 0} b_{k-r} c_{l+r} = 0 \mod p$, so $a_{k+l} \equiv b_k c_l \mod p \not\equiv 0 \mod p$ X

Corollary: let $a(x) \in \mathbb{Z}[x]$ $a(x)$ has no proper factorisation over $\mathbb{Z} \Rightarrow a(x)$ has no proper factorisation over $\mathbb{Q}$

Proof: Suppose $\deg a(x) = n$ $a(x) = \beta(x)\gamma(x)$, $\beta, \gamma \in \mathbb{Q}[x]$

Multiply by LCM $= M$ all coeffs of $\beta(x)$ st $M\beta(x) \in \mathbb{Z}[x]$ and $N\gamma(x) \in \mathbb{Z}[x]$

$N =$ LCM of all coeffs of $\gamma(x)$

so $MN\, a(x) = [M\beta(x)][N\gamma(x)] = b(x)c(x)$, $b = M\beta$ $c = N\gamma$

Let $A = C(a)$, $B = C(b)$, $C = C(c)$

$a(x) = Aa_0(x)$, $b(x) = Bb_0(x)$, $c(x) = Cc_0(x)$

$MNAa_0(x) = BCb_0(x)c_0(x)$ By Gauss' lemma $C(b_0c_0) = 1$

$\Rightarrow MNA = BC \Rightarrow a_0(x) = b_0(x)c_0(x)$

$a(x) = Ab_0(x)c_0(x)$ This is a proper factorisation over $\mathbb{Z}X$.

so now Eisensteins (over $\mathbb{Q}$)

If $a(x) = a_nx^n + \dots + a_0 \in \mathbb{Z}[x]$ and for some prime p:

i) $a_n \not\equiv 0 \bmod p$

ii) $a_r \equiv 0 \bmod p$ $r<n$

iii) $a_0 \not\equiv 0 \bmod p^2$

Then $a(x)$ is irreducible over $\mathbb{Q}$.

Factorisation of Cyclotomic Polynomials

Solns to $\boxed{x^n - 1 = 0}$ over $\mathbb{C}$ are $x = \exp\left(\frac{2\pi i}{n}\right)$ so $y^r = \exp\left(\frac{2\pi i r}{n}\right)$ are roots.

forms a cyclic group generated by y.

$$x^n - 1 = \prod_{r=0}^{n-1}(x - y^r)$$

NB: $\text{ord}\, y^r = d = \frac{n}{\text{LCM}(n,r)}$

Write $C_d(x) = \prod_{\text{ord}\, y^r = d}(x - y^r)$

$$\therefore x^n - 1 = \prod_{d = d/n}\left[\prod_{\text{ord}\, y^r = d}(x - y^r)\right] = \prod_{d/n} C_d(x)$$

ⓔⓖ $x - 1 = C_1(x)$

$x^2 - 1 = C_1(x)C_2(x) = (x-1)C_2(x) = (x-1)(x+1) \Rightarrow C_2(x) = x+1$

$x^3 - 1 = C_1(x)C_3(x) = (x-1)(x^2+x+1)$

NB: $\boxed{C_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \dots + x + 1 \quad \text{irreducible}}$

$$x^4-1 = C_1(x)C_2(x)C_4(x) = (x^2-1)C_4(x) \Rightarrow C_4(x) = x^2+1$$

$$x^6-1 = C_1(x)C_2(x)C_3(x)C_6(x) = \cancel{[illegible]}$$

$$(x^3-1)(x+1)C_6(x) \Rightarrow x^3+1 = (x+1)C_6(x) \Rightarrow C_6 = x^2-x+1$$

NB: $C_6(x) = C_3(-x)$ also $C_8 = x^4+1$

$$x^{24}-1 = C_1(x)C_2(x)C_3(x)C_4(x)C_6(x)C_8(x)C_{12}(x)C_{24}(x)$$

first find C_{12}

$$x^{12}-1 = (C_1C_2C_3C_6)C_4C_{12} = (x^6-1)(x^2+1)C_{12} \Rightarrow (x^6+1) = (x^2+1)C_{12}$$

$$C_{12} = x^4 \cancel{+2x^3} - x^2 \cancel{+2x} + 1 = x^4 - x^2 + 1$$

$$x^{24}-1 = (x^{12}-1)C_8C_{24} \Rightarrow C_{24} = \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1 = C_3(-x^4$$

Can also factorise $x^n+1 = \frac{x^{2n}-1}{x^n-1}$

$$x^{15}-1 = C_1C_3C_5C_{15} = (x^5-1)C_3C_{15}$$

$$\ x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

$$\Rightarrow C_3C_{15} = x^{10}+x^5+1 \Rightarrow C_{15} = x^2+x+1 \overline{\big) x^{10}+x^5+1}$$

$$\frac{x^n+1}{x^q+1} = x^{n-q} - x^{n-2q} + x^{n-3q} - x^{n-4q} + \dots + 1$$

Algebra 4 - Sheet 8 ⓅⒸ

16th March 2012

② $\mathbb{F}_5[x] / (x^2+x+2) \xrightarrow{\simeq} \mathbb{F}_5(x) / (y^2+4y+2)$

0 1 2 3 4

$\varphi(a+bx) = a+4by$ obviously linear so $\boxed{x=4y}$

$(4y)^2+4y+2 = 16y^2+4y+2 = y^2+4y+2$

Check φ preserves mult, ie

$\boxed{\varphi[(a+bx)(c+dx)] = \varphi[a+bx]\,\varphi(c+dx)}$ $x^2=-x-2$

$\varphi(ac+(ad+bc)x+bdx^2) = \varphi(ac+(ad+bc)x - bdx - 2bd)$

$= \varphi((ac-2bd)+(ad+bc-bd)x)$

$\Rightarrow \varphi(a+bx)(c+dx) = ac-2bd+4(ad+bc-bd)y$

other way $y^2=-4y-2$

$\varphi(a+bx)\varphi(c+dx) = (a+4by)(c+4dy) = ac+4bcy+4ady+16bdy^2$

$= (ac-2bd)+4(ad+bc-bd)y$

NOT $\mathbb{F}_5[x] / (x^2+x+2) = C_{24}$ unless $\left(\mathbb{F}_5[x] / (x^2+x+2)\right)^* = C_{24}$

---

③ i) $\mathbb{F}[x] / (x^2-1) \cong \mathbb{F}\times\mathbb{F}$ provided $2\neq 0$ in $\mathbb{F}$ ie 2^{-1} exists in $\mathbb{F}$.

$e_1 = \frac{1+x}{2}$, $e_2 = \frac{1-x}{2}$: $e_1+e_2=1$ $e_1e_2=0$ $e_1^2 = \frac{1+2x+x^2}{4} = \frac{2+2x}{4} = \frac{1+x}{2} =$

An element is idempotent when $e^2=e$

Obvious idempotents in $\mathbb{F}\times\mathbb{F}$ $\epsilon_1=(1,0)$ $\epsilon_2(0,1)$ $\epsilon_1^2=\epsilon_1$ $\epsilon_2^2=\epsilon_2$

$\epsilon_1+\epsilon_2=(1,1)=1$ $\epsilon_1\epsilon_2=0$

$\varphi : \mathbb{F}\times\mathbb{F} \longrightarrow \mathbb{F}[x]\big/_{x^2-1}$

$(a,b) = a\epsilon_1 + b\epsilon_2$ $\qquad$ $\varphi(a,b) = a\varphi(\epsilon_1) + b\varphi(\epsilon_2)$

$\epsilon_1 \to e_1$ $\qquad$ $= \frac{a(1+x)}{2} + \frac{b(1-x)}{2}$

$\epsilon_2 \to e_2$

$= \left(\frac{a+b}{2} , \frac{a-b}{2}\right)$

ii) $\mathbb{R}[x]\big/_{x^2+a} \cong \mathbb{R}\times\mathbb{R}$ when $a<0$

Write $a=-b$ $\quad b>0$

Put $y = \frac{x}{\sqrt{b}} = \frac{x}{\sqrt{-a}}$

$\mathbb{R}[x]\big/_{x^2+a} \simeq \mathbb{R}[x]\big/_{x^2-b} \cong \mathbb{R}[x]\big/_{x^2-(\sqrt{b})^2}$

$= \mathbb{R}[y]\big/_{y^2-1} \cong \mathbb{R}\times\mathbb{R}$ by above.

$\mathbb{R}[x]\big/_{x^2+a}$ $\quad a>0$ $\quad$ Only nonzero idempotent is 1

Make a transformation $y = \frac{x}{\sqrt{a}}$

$\mathbb{R}[x]\big/_{x^2+a} \cong \mathbb{R}[y]\big/_{y^2+1} \cong \mathbb{C}$

Algebra 4

16th March '12

Finite Subgroups of $\mathbb{F}^*$

$\mathbb{F}$ field. $\mathbb{F}^* = \{x \in \mathbb{F} : x \neq 0\}$ $\mathbb{F}^*$ forms a group under mult.

Thm: if $G \subset \mathbb{F}^*$ is a finite subgroup then G is cyclic

Prop: Let $\mathbb{F}$ be a field, p a prime and $G \subset \mathbb{F}^*$ a subgroup with $|G| = p^n$. Then $G \cong C_{p^n}$

Proof: Suppose $G \not\cong C_{p^n}$. If $x \in G$ then the only possibilities for $\operatorname{ord}(x)$ are $1, p, p^2 \ldots p^{n-1}$ (by Lagrange)

Let $e = \max\{r : 0 \leq r \leq n-1$ st $\exists x \in G$ $\operatorname{ord}(x) = p^r\}$

so $\exists\, x \in G : \operatorname{ord}(x) = p^e$ $e < n$. So every other element $y \in G$ satisfies $\boxed{y^{p^e} = 1}$ so $\forall y \in G$ g satisfies the eqn $\boxed{g^{p^e} = 1}$

Thus a polynomial eqn$/_{\mathbb{F}}$ of degree p^e so $\exists$ at most p solutions and every element $g \in G$ is a solution

so $|G| \leq p^e$ But $|G| = p^n$ contradiction since $e < n$.

Hence G has an element of order p^n. Hence $G \cong C_{p^n}$ $\square$

Corollary: Let $\mathbb{F}$ be a field $G \subset \mathbb{F}^*$ a finite subgroup Then G is cyclic.

Proof: Write $|G| = p_1^{n_1} p_2^{n_2} \ldots p_m^{n_m}$ where $p_1 \ldots p_m$ are distinct primes. If $m = 1$ shown that G is cyclic. Prove by induction on m that G is cyclic. Induction base is Ok. So assume proved for $m-1$ and let $|G| = p_1^{n_1} \ldots p_m^{n_m}$ as abo

By Sylow for each i $\exists$ subgroup $G_i \in G$ with $|G_i| = p^{n_i}$

In particular each G_i is cyclic. If $i \neq j$ $G_i G_j = G_j G_i$;

so $G' = G_1 \cdot \ldots \cdot G_{m-1}$ $|G'| = p_1^{n_1} \ldots p_{m-1}^{n_{m-1}}$ By induction G' is cyclic.

$G = G' \cdot G_m$

$|G_m| = p_m^{n_m}$ is cyclic also (by induction base).

$G' G_m = G_m G'$ ($\mathbb{F}^*$ is abelian)

$G' \cap G_m = \{1\}$ coprime orders.

$G \cong G' \times G_m$ Product of cyclic groups of coprime order
Hence cyclic. $\square$.

Corollary: Let p be a prime.
Then $\mathrm{Aut}(C_p) \cong C_{p-1}$

Proof: $C_p = \{1, x, \ldots, x^{p-1}\}$ $x^p = 1$

$\mathrm{Aut}(C_p) = \{\varphi_r ; r \text{ coprime to } p\} = \{\varphi_1, \varphi_2, \ldots, \varphi_{p-1}\}$ because p is prime.

Let $\mathbb{F}_p$ = field with p elements.

$\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ $\left.\begin{array}{l} \mathbb{F}_p^* \longrightarrow \mathrm{Aut}(C_p) \\ r \longmapsto \varphi_r \end{array}\right\}$ is a group isomorphism.

But $\mathbb{F}_p^*$ is finite so by above

$\mathbb{F}_p^* \cong C_{p-1}$ Hence $\mathrm{Aut}(C_p) \cong C_{p-1}$ $\square$.

$(\mathbb{Z}/n)^*$?

$\mathbb{Z}/n$ is the ring of residues mod n.

$(\mathbb{Z}/n)^* = \{x \in \mathbb{Z}/n : \exists y \in \mathbb{Z}/n \quad xy = 1\}$

$(\mathbb{Z}/n)^*$ is the unit group of invertible elements in $\mathbb{Z}/n$

When $n = p$ is prime $(\mathbb{Z}/p)^* \equiv \mathbb{F}_p^* \cong C_{p-1}$

What happens when n is composite?

Defn: Define $\Phi(n) = \left|(\mathbb{Z}/n)^*\right|$ = no. of invertible residues mod n.

$\nearrow$ Eulers Phi Function.

How to compute $\Phi(n)$

Rule 1: If m,n are coprime then $\Phi(mn) = \Phi(m)\Phi(n)$

Proof: Consider the following mappings.

$$\nu : \mathbb{Z}/_{mn} \longrightarrow \mathbb{Z}/_{m} \times \mathbb{Z}/_{n}$$

$$\nu\left[[x]_{mn}\right] = \left([x]_{m}, [x]_{n}\right)$$

ν is additive and multiplicative (easy!)

If m,n are coprime then ν is injective. Why?

Suppose $\nu([x]_{mn}) = (0,0)$

This means $x = km$ for some k $\nearrow$

$\nwarrow$ This 0 means $x = ln$ for some l.

$km = ln$

$km = ln$ because m,n are coprime so we must have

$k = \lambda n$, $l = \mu m$

$x = \lambda mn$ so $[x]_{mn} = 0$

$|\mathbb{Z}/_{mn}| = mn$ $\quad |\mathbb{Z}/_{m} \times \mathbb{Z}/_{n}| = mn$ Because φ is injective it is surjective.

So $\mathbb{Z}/_{mn} \cong \mathbb{Z}/_{m} \times \mathbb{Z}/_{n}$ so $(\mathbb{Z}/_{mn})^* \cong (\mathbb{Z}/_{m})^* \times (\mathbb{Z}/_{n})^*$ $\square$. So

so $\Phi(mn) = \Phi(m)\Phi(n)$ if m,n coprime

Rule 2: If $n = p_1^{e_1} \dots p_k^{e_k}$ where $p_1 \dots p_k$ distinct primes.

then $\Phi(n) = \Phi(p_1^{e_1}) \dots \Phi(p_k^{e_k})$

So it suffices to compute

$\Phi(p^m)$ when p is prime.

Rule 3: If p is prime $\Phi(p^m) = (p-1)p^{m-1}$

Proof: The non-invertible elements of $\mathbb{Z}/p^m$ are the residues which are divisible by p. The invertible elements are those which are nonzero mod p.

$$\mathbb{Z}/_{p^m} \xrightarrow{\varphi} \mathbb{Z}/_{p}$$

$$[x]_{p^m} \longmapsto [x]_p$$

Non invertible elements $= \ker \varphi$ $\quad |\ker \varphi| = p^{m-1}$

Invertible elements belong to cosets

$1 + \ker(\varphi),\ 2 + \ker(\varphi), \ldots, (p-1) + \ker(\varphi)$

Each coset has p^{m-1} elements so

$$\Phi(p^m) = (p-1)p^{m-1} \quad \square$$

Algebra 4 20th March 12

$\Phi(n) = |(\mathbb{Z}/n)^*|$ Euler Phi Function

i) Number of invertible elements in $\mathbb{Z}/n$

ii) Number of generators of C_n

iii) Order of $Aut(C_n)$

1) $\Phi(mn) = \Phi(m)\Phi(n)$

2) If $n = p_1^{e_1} \cdots p_k^{e_k}$ where $p_1 \cdots p_k$ distinct primes

$$\Phi(n) = \prod_{i=1}^{k} \Phi(p_i^{e_i})$$

3) $\Phi(p^m) = (p-1)p^{m-1} = (1-\frac{1}{p})p^m$

4) $\Phi(n) = \left[\prod_{i=1}^{k}(1-\frac{1}{p_i})\right]n$ where $p_1 \cdots p_k$ are distinct primes dividing n.

$\boxed{\Phi(100) = 40}$ $100 = 2^2 \cdot 5^2$

$\Phi(100) = \Phi(2^2)\Phi(5^2)$ $2 \times 4 \times 5 = 40$

$\Phi(360)$ $360 = 2^3 \cdot 3^2 \cdot 5$

$\Phi(360) = \Phi(2^3)\Phi(3^2)\Phi(5) = 4 \times 6 \times 4 = 96.$

n	G	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	✓
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}	✓
2	C_{12}, $C_6 \times C_2$, D_{12}, D_6^*, A_4	✓
3	C_{13}	✓
4	C_{14}, D_{14}	✓
15	C_{15}	✓
16	Ä	
7	C_{17}	✓
8	Involved	
9	C_{19}	✓
0	C_{20}, $C_2 \times C_{10}$, D_{20}, D_{10}^*, $G(20)$	
21	C_{21} $G(21)$	✓
2	C_{22}, D_{22}	✓
3	C_{23}	✓
4	Involved	
5	C_{25}, $C_5 \times C_5$	✓

$C_{20}^{*} = C_4 \times C_5$

$C_2 \times C_{10} = C_2 \times C_2 \times C_5$

Thm

If p is prime then there are exactly 2 distinct groups of order p^2, namely C_{p^2} and $C_p \times C_p$.

Proof: For $p=2$ we already know this

First prove lemma 1: If $|G| = p^n$ (p prime) then

$Z(G)$ is non trivial. $Z(G) = \{x \in G : \forall y \in G \ xy = yx\}$

Proof: Let G act on itself by conjugation.

$G \times G \longrightarrow G$.

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

The fixed point set under this action is precisely $Z(G)$

$gxg^{-1} = x \Leftrightarrow xg = gx$. If $gxg^{-1} = x \ \forall g$ then $x \in Z(G)$ & conversely.

So. $Z(G) = G^G$ so $|Z(G)| \equiv |G| (\mathrm{mod}\ p)$

But $|G| \equiv 0 \mod p$ so $|Z(G)| = 0 \mod p$.

If $Z(G) = \{1\}$ then would get $|Z(G)| \equiv 1 \mod p$, so $Z(G) \neq \{1\}$ □

Lemma 2: If G is nonabelian then $G/Z(G)$ is not cyclic.
Proved as exercise.

$*: G \times X \to X$ ASIDE

$X^G = \{x \in X \ \forall g \in G \ g \cdot x = x\}$ so G^G is defined

Corollary: If $|G| = p^2$ then G is abelian

Proof: If G is nonabelian $Z(G) \neq 1$ by lemma 1.

so $|Z(G)| = p$ (can't be p^2 otherwise $G = Z(G)$ } is abelian)

Hence $|G/Z(G)| = p$ so $G/Z(G)$ is cyclic (contradicts lemma 2

Hence G abelian □.

Proof: $|G| = p^2 \Rightarrow G$ abelian.

If $G \not\cong C_{p^2}$ then every $g \in G$ satisfies $g^p = 1$

Method 1: Since G is abelian, write additively.

$\forall g \in G \quad \underbrace{g + \cdots + g}_{p} = 0 \qquad p \cdot g = 0.$

Got a vector space $/\mathbb{F}_p$

Use basis then $G \cong \mathbb{F}_p \oplus \mathbb{F}_p \cong C_p \times C_p$

Method 2: Let $x \in G$ $\text{ord}(x) = p$

Let $y \in G - \{1, x, \ldots, x^{p-1}\}$ so $\text{ord}(y) = p$

Put $K = \{1, x, \ldots, x^{p-1}\}$ $\quad Q = \{1, y, \ldots, y^{p-1}\}$

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

$K \trianglelefteq G$ because G abelian. so $G \cong K \rtimes_{\varphi} Q$

$\varphi : \underset{C_p}{\overset{}{Q}} \to \text{Aut}(K) = C_{p-1}$ $\quad$ φ must be trivial

$G \cong K \times Q \cong C_p \times C_p \quad \square.$

Groups to vector spaces...

G abelian group written multiplicatively

$g \cdot h = h \cdot g \quad 1 \cdot g = g$

$\hat{G}$ same elements except you write $g \to \hat{g} \qquad \hat{1} = 0$

Instead of $\cdot$ I write $+$.

$g \cdot h \to \hat{g} + \hat{h}$

$h \cdot g \to \hat{h} + \hat{g}$

Assume in G that

$g^p = 1$ for all $g \in G$.

$\underbrace{\hat{g} + \hat{g} + \dots + \hat{g}}_{p} = 0$ $\quad p\hat{g} = 0$ $\quad$ This is exactly what it means to be a vector space $/\mathbb{F}_p$.

If $|G| = 20$, $\quad G \cong C_5 \rtimes C_4$ or $\quad G \cong C_5 \rtimes (C_2 \times C_2)$

There are 3 groups of type $C_5 \rtimes C_4$

$C_5 = \{1, x, x^2, x^3, x^4\}$ $\quad C_4 = \{1, y, y^2, y^3\}$

$Aut(C_5) \cong C_4 = \{1, \varphi_2, \underset{\varphi_4}{\underset{\shortparallel}{\varphi_2^2}}, \underset{\varphi_3}{\underset{\shortparallel}{\varphi_2^3}}\}$

Get 4 homos $C_4 \to Aut(C_5)$

$h_0: h_0(y) = Id \longleftrightarrow C_5 \times C_4$

$h_1: h_1(y) = \varphi_2 \longleftrightarrow x^5 = y^4 = 1, \ yxy^{-1} = x^2$, $\cong$

$h_2: h_2(y) = \varphi_4 \longleftrightarrow D_{10}^* = \{x^5 = y^4 = 1, \ yxy^{-1} = x^4 = x^{-1}\}$

$h_3: h_3(y) = \varphi_3 \longleftrightarrow x^5 = y^4 = 1 \quad yxy^{-1} = x^3$ $\quad$ $\cong$ swap $y \leftrightarrow y^3$

Difficulties with groups of order 18

$|G| = 18 = 2 \cdot 3^2$

Usual Sylow counting gives a normal subgroup K. $|K| = 9$ and a subgroup Q. $|Q| = 2$

$$G \cong K \rtimes Q \left\{ \begin{array}{l} C_9 \rtimes_\varphi C_2 \\ (C_3 \times C_3) \rtimes_\varphi C_2 \end{array} \right.$$

$Aut(C_9) \cong C_6 = \{\varphi_1, \underset{\alpha}{\underset{\shortparallel}{\varphi_2}}, \underset{\alpha^2}{\underset{\shortparallel}{\varphi_4}}, \underset{\alpha^3}{\underset{\shortparallel}{\varphi_8}}, \underset{\alpha^4}{\underset{\shortparallel}{\varphi_7}}, \underset{\alpha^5}{\underset{\shortparallel}{\varphi_5}}\}$ $\quad \alpha^6 = Id$

$C_2 \longrightarrow \mathrm{Aut}(C_9)$ $\quad y \to 1 \leftrightarrow C_9 \times C_2$

$\overset{\shortparallel}{\{1,y\}}$ $\quad y \to \alpha^3 \longleftrightarrow D_{18}$

Problem arises in describing $\mathrm{Aut}(C_3 \times C_3)$

Write C_3 additively. Then $\mathrm{Aut}(C_3 \times C_3) \longleftrightarrow GL_2(\mathbb{F}_3)$ = Invertible 2×2 matrices over $\mathbb{F}_3$

$|GL_2(\mathbb{F}_3)| = 48 = 2^4 . 3$

To complete classification of groups of order 18 we need

1) Find all $A \in GL_2(\mathbb{F}_3)$ $\quad A^2 = IA$.

2) Each such A gives a homo $C_2 \to \mathrm{Aut}(C_3 \times C_3)$

3) Decide which groups are then isomorphic.

ⓔⓖ $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\quad A^2 = 1$

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

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

$C_3 \times C_3 \longleftrightarrow \mathbb{F}_3 \oplus \mathbb{F}_3$

$\alpha : C_3 \times C_3 \to C_3 \times C_3$ preserves mult and is bijective $\Bigg\}$ $\alpha : \mathbb{F}_3 \oplus \mathbb{F}_3 \to \mathbb{F}_3 \oplus \mathbb{F}_3$ α preserves addition. Then α is described by a matrix.

$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\quad$ basis.

$\alpha(e_1) = ae_1 + ce_2$

$\alpha(e_2) = be_1 + de_2$

$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\quad a, b, c, d \in \mathbb{F}_3$

α bijective $\Longleftrightarrow$ $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$

Algebra 4 Sheet 9 (PC) 23rd March 12

$\frac{\mathbb{Q}[x]}{x^2-2} \not\cong \frac{\mathbb{Q}[y]}{y^2+2}$ can't just say $2 \neq -2$.

$a+bx$ $x^2 = 2$ $c+dy$ $y^2 = -2$

$a, b \in \mathbb{Q}$ $c, d \in \mathbb{Q}$

$\varphi : \frac{\mathbb{Q}[x]}{x^2-2} \longrightarrow \frac{\mathbb{Q}[y]}{y^2+2}$ $\varphi(1) = 1$

$\varphi(a+bx) = \varphi(a) + \varphi(b)\varphi(x) = a + b\varphi(x)$ ~~$\varphi(x) = -2$~~

$\varphi(x) = c+dy$ $\varphi(x)^2 = \varphi(x^2) = \varphi(2) = 2$

$(c+dy)^2 = 2$ $(c^2 + d^2y^2) + 2cdy = 2\,1$

$c^2 - 2d^2 = 2$ $2cd = 0$ so either c or d

Either $c = 0$ when $-2d^2 = 2$ contradiction or $c \in \mathbb{Q}$ contradiction

$d = 0$ when $c^2 = 2$

Algebra4 Exam 2011

4) $|G| = 56 = 7 \cdot 8 = 2^3 \cdot 7$

Show that either

i) G has a normal subgroup of order 7 ← larger prime first

or ii) " " " " " " 8

N_7 = no. of subgroups of order 7.

$N_7 \equiv 1 \bmod 7$ $\quad N_7 = 1, 8$ or ≥ 15

If $N_7 = 15$, $\exists$ at least $15 \times 6 = 15 \times (7-1) = 90$ elements $\therefore \times$.

if $N_7 = 8$ we get exactly $8 \times 6 = 48$ elements of order 7.

$56 - 48 = 8$

Know $\exists$ at least one subgroup of order 8 so there is exactly one

So either $N_7 = 1$ and G has a unique (and $\therefore$ normal) Subgrp of ord

or $N_7 = 8$ and $N_2 = 1$ and G has a " " " " " "

1

3) Classify groups of order $1075 = 43 \times 25 = 43 \cdot 5^2$

$N_{43} \equiv 1 \pmod{43}$ so $N_{43} = 1$ or $N_{43} \geq 44$

If ≥ 44 get at least 44×42 elements

$N_{43} = 1$ Let K be the normal subgroup of order 43

Q be a subgroup of order $25 = 5^{2}$

Either $G \cong K \rtimes_{\varphi} Q$ (Recog crit)

$C_{43} \rtimes_{\varphi} C_{25}$ or $C_{43} \rtimes_{\varphi} (C_5 \times C_5)$ $\quad \mathrm{Aut}(C_{43}) = C_{42}$

$5 \nmid 42$ so only get trivial homos $\varphi \to \mathrm{Aut}(C_{43})$

So either $G \cong C_{43} \times C_{25} \cong C_{1075}$

or $G \cong C_{43} \times C_5 \times C_5 \cong C_{215} \times C_5$

5) x^2+2x+2 irred$/\mathbb{F}_3$ $\qquad ax^2+bx+c$ irred $/\mathbb{F}$

$4-8=-4=-1=2$ $\qquad \iff b^2-4ac$ not a square in $\mathbb{F}$

2 is not a square in $\mathbb{F}_3$ so x^2+2x+2 is irred.

$$\left|\mathbb{F}_3[x] \Big/ x^2+2x+2\right| = 9 \qquad \left(\mathbb{F}_3[x] \Big/ x^2+2x+2\right)^* = 8 = (9-1)$$

Finite subgroup of a field so it must be C_8.

x

$x^2 = -2x-2 = x+1$

$x^3 = x(x+1) = x^2+x = -x-2 = 2x+1$

$x^4 = x(2x+1) = 2x^2+x - -x^2+x = 2x+2+x = 2$

$x^8 = 2^2 = 1$ $\qquad$ x generates

6) $x^{18}-2x^9-3 = (x^9+1)(x^9-3) = (x^9-3)(x^3+1)(x^6-x^3+1)$

$$= \underset{\substack{\uparrow \\ \text{irred by} \\ \text{eisenstein}}}{(x^9-3)}(x+1)\underbrace{(x^2-x+1)(x^6-x^3+1)}_{\text{irred because cyclotomic}}.$$

How $\boxed{\text{not}}$ to apply eisenstein

$x^{100}+3x+5$

$1 \not\equiv 0 \bmod 3$

$3 \equiv 0 \bmod 3$ — $5 \not\equiv 0 \bmod 3$

$5 \not\equiv 0 \bmod 3^2$

$x^5-5x^4+10x^3-10x^2+5x-1-3$

$(x-1)^5-3$ irred by eisenstein $p=3$