7202 Algebra 4: Groups and Rings Notes

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

11/01/11

Revision

Def-n $\mathcal{G} = (G, *, e) \to$ group

set, element of set: $e \in G$

0) $*: G * G \to G$ mapping

1) $a*(b*c) = (a*b)*c \quad \forall a, b, c \in G$

Identity → 2) $a * e = e * a = a \quad \forall a \in G$

нейтральный элемент

3) $\forall a \ \exists \bar{a}: \ a * \bar{a} = e = \bar{a} * a$ → Inverses

associative; св-ва действия *

In practice: we use either:

- Multiplicative convention → правило

$$\begin{cases} * = \cdot \\ e = 1 \\ \bar{a} = a^{-1} \end{cases}$$

- Additive convention

$$\begin{cases} * = + \\ e = 0 \\ \bar{a} = -a \end{cases}$$

Note: used only when $a + b = b + a$ commutative

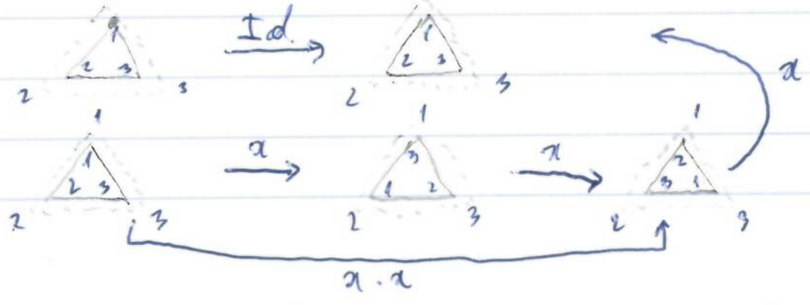
{We use this very little}, as most groups are not Abelian!}

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

циклическая группа

example 1 C_3 cyclic group of order 3

Symmetries of 1-sided Δ.



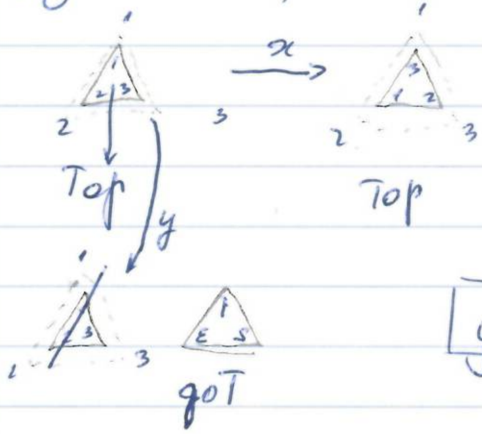
conclusion : $\boxed{1, x, x^2 \quad x^3 = 1}$ ← Pres. of group

C_3	1	x	x^2
1	1	x	x^2
x	x	x^2	$\cancel{x^3}\ 1$
x^2	x^2	$\cancel{x^3}\ 1$	x

← "Latin square"

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

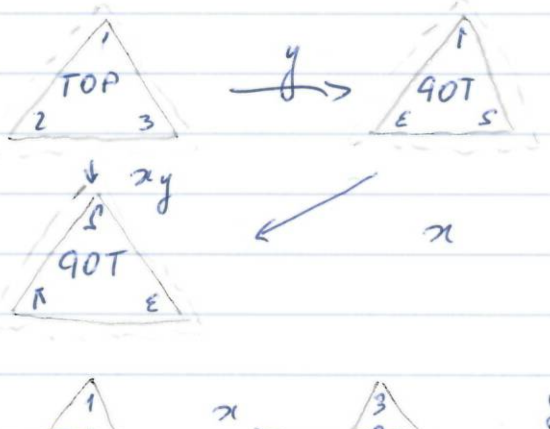
2) Symmetries of a 3-sided Δ

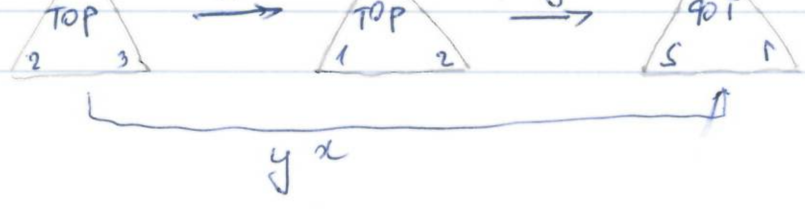


$\boxed{x^3 = 1}$

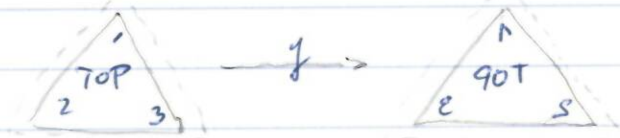
$\boxed{y^2 = 1}$

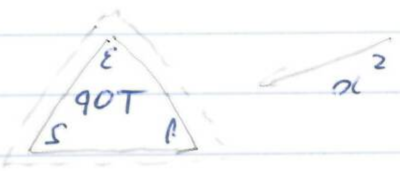
$f \circ g$ = first g then f
xy = first y then x





, so $yx \neq xy$





So $yx = x^2y$

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

D_6	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	$\cancel{yx}$ x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

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

Диэдральная группа

yx^2 we know $yx = x^2y$

$\underline{yx^2} = yxx = x^2yx = x^2 \cdot x^2y = xy$

$(yx)y = x^2y \cdot y = x^2$

$(yx^2)y =$

<u>So far</u>

C_3 = group of symmetries of 1 sided equilatared Δ is abilian

D_6 = — " ——— 2 ——— " ———

$6 = 2 \times 3$ Non-abilian.

generalisation.

14/01/11

1) $C_n = \{1, x, \dots, x^{n-1}\}$ $x^n = 1$ - cyclic group of order n

(•) x = rotation through $\frac{2\pi}{n}$ (anticlockwise)

(•) $x^{-1} = x^{n-1}$ (•) $x x^{n-1} = x^n = 1$

2) D_{2n} = dihedral group of order $2n = \{1, x, \dots, x^{n-1}, y, xy, \dots, x^{n-1}y\}$ $x^n = 1, y^2 = 1$

(•) x = rotate regular 2-sided n-gon through $\frac{2\pi}{n}$

TOP → TOP

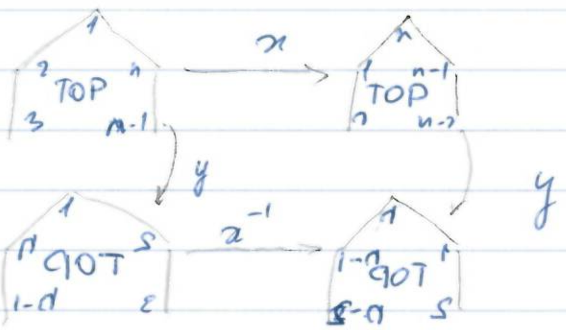
(•) y = flip about chosen vertex

TOP → ꟼOT

$x^n = 1$

$y^2 = 1$

Q. How do x, y interact?



this shows $\boxed{yx = x^{-1}y}$, alternatively expressed $\boxed{yx = x^{n-1}y}$

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

$D_{2n} = \{1, x, \dots, x^{n-1}, xy, \dots, x^{n-1}y\}$

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

группа кватерниона

Quaternion group of order 8 : Q_8

$\{1, i, -1, -i\}$

$i^2 = -1$, $i^3 = -i$, $i^4 = 1$ $\quad \subset \mathbb{C}$

This is another model for C_4

$Q_8 = \{1, i, -1, -i, j, -j, k, -k\}$ W. R. Hamilton 1850

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

$k = ij = -ji$

Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	$+j$
$-i$	$-i$	i	$+1$	-1	$-k$	$+k$	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	$+j$	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

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

как определить, что операция ассоциативна?

Q_8 nonabelian group of order 8

D_8 nonabelian gr. of order 8

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

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

C_4	1	x	x^2	x^3
1	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

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Conclusion:

существенно

Q_8 & D_8 are essentially different

гомоморфизм групп

отображение

Def-n. Let $\mathcal{G} = (G, \circ, 1_G)$, $\mathcal{H} = (H, *, 1_H)$ } be groups

say that a mapping $f : G \to H$ is a **group homomorphism** when

$$f(g_1 \circ g_2) = f(g_1) * f(g_2) \quad \text{for all } g_1, g_2 \in G$$

□

Ex. $\mathbb{R} = (\mathbb{R}, +, 0)$

$\mathbb{R}_+ = (\mathbb{R}_+, \cdot, 1)$ $\qquad \mathbb{R}_+ := \{x \in \mathbb{R} : x > 0\}$

1) $\exp : \mathbb{R} \to \mathbb{R}_+$ is homomorphism,
as $\exp(x+y) = \exp(x)\exp(y)$

2) $\log : \mathbb{R}_+ \to \mathbb{R}$ is homomorphism
$\log(xy) = \log x + \log y$

3) $\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$

Def-n We write $G \cong H$ when $\exists$ **bijective homomorphism** $f : G \to H$

G and H are then **isomorphic**

Note that in D_8, $1, x^2y, xy, x^2y, x^3y$ are all self inverse whereas in Q_8 only $1, -1$ are self inverse

Elementary properties of homomorphism

$\begin{cases} G = (G, \circ, 1_G) \\ H = (H, *, 1_H) \end{cases}$

$f: G \to H$ group homomorphism

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

$f(x)^{-1}$ is inverse of element
$f^{-1}(x)$ is inverse function

$\therefore f(x)^{-1} f(x) = 1$
$f^{-1}(x) \circ f(x) = x$

Proof of (1)

$f(1_G) = f(1_G \cdot 1_G) = f(1_G) * f(1_G)$

multiply (on left) by $f(1_G)^{-1}$ → this is inverse of element $f(1_G)$ in H

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

$1_H = 1_H * f(1_G) = f(1_G)$ Q.E.D. (1)

Proof of (2)

$1_G = x \circ x^{-1} = x^{-1} \circ x$

$f(1_G) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$

But $f(1_G) = 1_H$

So $f(x) * f(x^{-1}) = 1_H$

Similarly $f(x^{-1}) * f(x) = 1_H$

So $f(x^{-1}) = (f(x))^{-1}$ Q.E.D.

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

Proof of (3)

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

Let $h_1, h_2 \in H$

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

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

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

f is homomorphism

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

But f is injective

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

Application: $Q_8 \not\cong D_8$

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

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

② f ~~introduce~~ induces a mapping
$f : S(G) \to S(K)$

Let $f^{-1} : S(K) \to S(G)$

[i.e. $f : S(G) \to S(K)$ is bijective with ~~[illegible]~~ inverse
$f^{-1} : S(K) \to S(G)$]

If $Q_8 \cong D_8$

<u>Then</u> $\exists$ bijection
$S(Q_8) \to S(D_8)$

<u>But</u> $|S(Q_8)| = 2$ $\quad |S(D_8)| = 6$

<u>so</u> $Q_8 \not\cong D_8$ Q.E.D.

почему если
уравнение-finite to $r \geq \infty$
?

generalisation

→ ~~Def-n.~~

$$\boxed{\begin{array}{l}\text{Let } G \text{ be a finite group, and} \\ g \in G \\ \operatorname{ord}(g) = \min\{ r \geq 1 : g^r = 1\} \quad r \in \mathbb{N}\end{array}}$$
□

<u>e.g.</u> $D_6 = \{1, x, x^2, y, xy, x^2y\}$
$\operatorname{ord}(1) = 1$
$\operatorname{ord}(x) = 3$
$\operatorname{ord}(x^2) = 3$
$\operatorname{ord}(y) = 2$
$\operatorname{ord}(xy) = 2$
$\operatorname{ord}(x^2y) = 2$ $\qquad \operatorname{ord}(g) \mid |D_6|$ where $g \in D_6$
почему?

$\nu_n(G) = |\{ g \in G : \operatorname{ord}(g) = n\}|$

<u>e.g.</u> for $G = D_6$
$\nu_1(D_6) = 1, \ \nu_2(D_6) = 3, \ \nu_3(D_6) = 2, \ \nu_n(D_6) = 0$ for $n \geq 4$

$D_8 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$
orders 1 4 2 4 2 2 2 2

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

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

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

To Do exercises 1 & 2.

You need to prove:

Prop. Let $f: G \to K$ be a bijective homomorphism

Then f induces a bijection

$f: G(n) \to K(n)$ for each n

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

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

so $\nu_n(G) = |G(n)|$ $\quad \nu_n(K) = |K(y)|$

so ... $\nu_n(G) = \nu_n(K)$

~~Directly~~

NFE **Prop**: if [G & K are isomorphic (G & K are groups)] $\Rightarrow$ [$\text{ord}\, g = \text{ord}\, f(g)$]

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

Proof: в отделе практики.

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

Direct product of groups

Def-n

$$\boxed{\begin{array}{l} G = (G, \cdot, 1_G) \qquad H = (H, \circ, 1_H) \\ G \times H = (G \times H, *, (1_G, 1_H)) \\ (g_1, h_1) * (g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2) \end{array} \Bigg\} \text{ is a group itself}}$$

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

$$\{(1,1)\ (x,1)\ (x^2,1)\ (1,x)\ (x,x)\ (x^2,x)\ (1,x^2)\ (x,x^2)\ (x^2,x^2)\}$$

1 3 3 3 3 3 3 3 3

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

1, 9, 9, 3, 9, 9, 3, 9, 9

$D_9(C_9) = 6 \qquad D_9(C_3 \times C_3) = 0.$

18.01.11

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

$ord(1) = 1 \quad ord(x) = 8 \quad ord(x^2) = 4 \quad ord(x^3) = 8$
$ord(x^4) = 2 \quad ord(x^5) = 8 \quad ord(x^6) = 4 \quad ord(x^7) = 8$

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

Question: $C_n = \{1, x, \dots, x^{n-1}\} \quad x^n = 1$
A typical element is x^r
what is $ord(x^r)$?

A: $\boxed{ord\, x^r = \dfrac{n}{HCF(n, r)}}$

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

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

Proof: 1) $ord(x) = n = \min\{r : x^r = 1\}$ and $x^N = 1$ then by def-n $n \leq N$ $\square$

2) Div. $N = qn + r \quad (0 \le r < n)$

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

But $x^n = 1$ so $x^r = 1$ and $0 \le r < n$

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

□ so $r = 0$ $N = qn$ QED

Prop. $\boxed{\operatorname{ord}(x^r) = \dfrac{n}{HCF(n, r)}}$

Proof. Write $\operatorname{ord}(x^r) = k$

so $(x^r)^k = 1$. So $x^{rk} = 1$

Hence n div. rk

ie. rk is a multiple of n

rk is obviously a multiple of r.

So rk is common multiple of n, r

when k is minimised $(x^r)^k = 1$ $(k \ge 1)$

then rk is lowest common ~~factor~~ multiple of n and r.

so $r \operatorname{ord} x^r = LCM(n, r) = \dfrac{nr}{HCF(n, r)}$

so $\operatorname{ord} x^r = \dfrac{n}{HCF(n, r)}$

QED

Prop. Let $f: G \to H$ $g: H \to K$ be a group homomorphism

Then $g \circ f: G \to K$ is also a homomorphism

Proof: $(g \circ f)(x_1 x_2) = g(f(x_1 x_2))$

$g(f(x_1) \cdot f(x_2)) = g[f(x_1)] g[f(x_2)]$

$= (g \circ f)(x_1) \cdot (g \circ f)(x_2)$ Q.E.D.

Automorphism group of G:

Def-n Let G be a group
A mapping $\alpha: G \to G$ is called **automorphism** of G, when
$$\boxed{\begin{array}{l}(1)\ \alpha \text{ is a homomorphism} \\ (2)\ \alpha \text{ is bijective.}\end{array}}$$

Def-n. $\boxed{Aut(G) = \{\alpha: G \to G \text{ s.t. } \alpha \text{ is an automorphism}\}}$

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

⇒ Proof:

1) Multiplication on $Aut(G)$:

- $Aut(G) \times Aut(G) \to Aut(G)$
  $(\alpha, \beta) \to \alpha \circ \beta$ composition and ~~is associative~~

~~$\Rightarrow \circ$ is binary operation~~

1) is it bijective? ✓
1) $\alpha \circ \beta(a) = \alpha \circ \beta(b) \Rightarrow a = b$ ✓
2) $\forall b \in G\ \exists a \in G$ s.t. $\alpha \circ \beta(a) = b$ ✓

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

Proof: composition of homomorphism is homomorphism
" — " — of bijective mapping is bijective □

$\Rightarrow \circ$ is binary operation

(closed) binary operation + a map in s.t. $S \times S \to S$

2) Identity: Take $Id_G: G \to G$

3) Inverses: If $\alpha: G \to G$ is bijective homomorphism, then
(1) α^{-1} is bijective and
(2) α^{-1} is a homomorphism

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

□ 4) Composition is always associative so get a group □

Example:

1) Determine $Aut(C_3)$

$C_3 = \{1, x, x^2\}$ $\quad x^3 = 1$ $\qquad$ Let $\alpha \in Aut(C_3)$

$\alpha(1) = 1$

$$\begin{array}{ccc} 1 & \xrightarrow{\alpha} & 1 \\ x & & x \\ x^2 & & x^2 \end{array}$$

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

Either $[\alpha(x) = x]$, then $\alpha(x^2) = \alpha(x)\alpha(x) = x \cdot x = x^2$
and then $\alpha = id$

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

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

проверка, что α является помимо bijective ещё и homomorphic

So

$$\begin{array}{ccc} & id & \\ 1 & \rightarrow & 1 \\ 2 & \rightarrow & 2 \\ 3 & \rightarrow & 3 \end{array} \qquad \begin{array}{ccc} & \tau & \\ 1 & \rightarrow & 1 \\ 2 & \searrow & 2 \\ 3 & \nearrow & 3 \end{array}$$

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

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

what is $\tau \circ \tau$

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

So $\tau \circ \tau = Id$

$Aut(C_3) \cong C_2$

	1	τ
1	1	τ
τ	τ	1

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

$1 \longrightarrow 1$ How many choices for $\alpha(x)$?

$x \quad x$ A: At most 4.

$x^2 \quad x^2$

$x^3 \quad x^3$

$x^4 \quad x^4$

Prop: It is enough to say where α takes x

Proof: Suppose

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

Let $\gamma : C_5 \to C_5$

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

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

$\gamma^3(x) = \gamma(\gamma^2(x)) = \gamma(x^4) = x^3$

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

So $\gamma^4 = \mathrm{Id}$

So $\mathrm{Aut}(C_5) \cong C_4$ generated by γ
$\gamma(a) = a^2$

→ а другие варианты разве не могут [illegible]? «Давай другую группу» [illegible]

[illegible] 21/01/11

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

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

First ~~conditions~~ observation: $\boxed{\varphi(a)^n = 1}$

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

Second observation: $\boxed{\varphi \text{ completely determined by value of } \varphi(a).}$

Proof: Typical element of C_n is a^r
$\varphi(a^r) = \varphi(a)^r$
So if you know $\varphi(a)$ then you know $\varphi(a^r)$ Q.E.D.

Pro-n

> Let $n \geq 2$
> $C_n = \{1, a, \dots, a^{n-1}\}$ $(a^n = 1)$
> H group, & let $h \in H$
>
> Then $\exists$ homomorphism $\varphi : C_n \to H$ with $\varphi(a) = h$
> iff $\mathrm{ord}(h)$ div n

$[\mathrm{ord}(h) \mid n]$

Proof

($\Rightarrow$) first observation

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

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

1) This is well defined (proved on 04.04 AP)

2) φ is a homomorphism as:

$$\varphi(a^r \cdot a^s) = \varphi(a^{r+s}) = h^{r+s} = h^r h^s = \varphi(a^r)\varphi(a^s)$$

QED

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

A: $\boxed{\varphi \text{ injective iff } \mathrm{ord}(h) = n}$

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

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

If φ is not injective, then $\varphi(a^r) = \varphi(a^s)$ for some r, s:

$0 \le r < s \le n-1$

Put $t = s - r$

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

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

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

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

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

it is inverse of the element!

$$1 = \varphi(a^t) = \varphi(a)^t$$

so $\mathrm{ord}\,\varphi(a) \le t < n$ contradiction Q.E.D ($\Leftarrow$)

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

$(1 = \varphi(1)), \varphi(a), \varphi(a)^2, \dots, \varphi(a)^{n-1}$ distinct

I know $\varphi(x)^n = \varphi(x^n) = 1$ so
$\text{ord}\,\varphi(x) \leq n$
If $\text{ord}\,\varphi(x) = k < n$ → contradiction $\varphi(x)^k = \varphi(1)$
so $\text{ord}(\varphi(x)) = n$ QED

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

standard def-n.
Let $0 \leq a \leq n-1$
Define $\varphi_a = C_n \to C_n$ by $\varphi_a(x) = x^a$

Previous discussion shows:
Pro-on:
If $\varphi : C_n \to C_n$ is a homomorphism
then $\varphi = \varphi_a$ for some $a : 0 \leq a \leq n-1$

почему не могут быть другие homomorphisms? которые не определены заданием [illegible]

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

т.е.

The question which really interests us is
Q: when is φ_a an automorphism $\varphi_a : C_n \xrightarrow{\cong} C_n$?

Prop: $\boxed{\varphi_a : C_n \to C_n \text{ is an automorphism} \iff a \text{ is coprime to } n.}$

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

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

$\varphi : C_n \to C_n$ is Bijective iff φ is injective

So φ_a is automorphism (it is already homomorphis by above)

iff φ_a is injective (by prop. above)

iff ord $x^a = n$

iff a, n coprime **QED**

Example 1) Calculate $Aut(C_7)$

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

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

$\varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$

$1, 2, 3, 4, 5, 6$ all coprime to 7

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

φ_0 is trivial homomorphism : $\varphi_0(x^r) = x^{0r} = 1$

($x^r \to 1$ for $\forall r$, not injective)

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

what is the group structure?

$\varphi_1 = Id$ (Always!!)

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

Put $\alpha = \varphi_3$

Calculate α^2 :

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

so $\alpha^2 = \varphi_2$

$\alpha^3(x) = \alpha(\alpha^2(x)) = \alpha(x^2) = \alpha(x)^2 = (x^3)^2 = x^6$

$\alpha^3 = \varphi_6$

$\alpha^4: \quad \alpha^4(x) = \alpha(\alpha^3(x))$
$= \alpha(x^6) = \cancel{x} x^8 = x^4$

$\underline{\alpha^4 = \varphi_4}$

$\alpha^5(x) = \alpha(\alpha^4(x)) = \alpha(x^4) = x^{12} = x^5$
$\alpha^5 = \varphi_5$

$\alpha^6(x) = \alpha(\alpha^5(x)) = \alpha(x^5) = x^{15} = x$
$\alpha^6 = \cancel{\varphi} id$

So $Aut(C_7) = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$
$1 = \varphi_1, \ \alpha = \varphi_3, \ \alpha^2 = \varphi_2, \ \alpha^3 = \varphi_6, \ \alpha^4 = \varphi_4, \ \alpha^5 = \varphi_5$

---

2) $\underline{Aut(C_9)}$ $\quad C_9 = \{1, x, \dots, x^8\}, \ x^9 = 1$

$Aut(C_9) = \{\varphi_a : a \text{ coprime to } 9\}$
$= \{\varphi_1, \varphi_2, \varphi_4, \varphi_5, \varphi_7, \varphi_8\}$
$\varphi_1 = Id$

Take $\beta = \varphi_2$
1) $\beta^2 = \varphi_4$
$\beta^3 = \varphi_8$
$\beta^4 = \varphi_7$
$\beta^5 = \varphi_5$
$\beta^6 = 1$

$Aut(C_9) \cong C_6 = \{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5\}$
$\beta \to \varphi_2, \ \beta^2 \to \varphi_4, \ \beta^3 \to \varphi_8, \ \beta^4 \to \varphi_7, \ \beta^5 \to \varphi_5$

3) $Aut(C_{15})$

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

$Aut(C_{15}) = \{\varphi_a : a \text{ coprime to } 15\}$

$\{\varphi_1, \varphi_2, \varphi_4, \varphi_7, \varphi_8, \varphi_{11}, \varphi_{13}, \varphi_{14}\}$

$\varphi_1 = Id$

Put $\alpha = \varphi_2$

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

$\alpha^3 = \varphi_8$

$\alpha^4 = Id$

почему ?

Put $\beta = \varphi_7$ $\beta^2 = \beta(\beta(x)) = \varphi_4 = \alpha^2$ × Rechoose

Put $\gamma = \varphi_{11}$

$\gamma^2 = \varphi_1$ $\gamma^2(x) = (x^{11})^{11} = x^{121} = x$

$$\begin{array}{cccccccc} \varphi_1, & \varphi_2, & \varphi_4, & \varphi_7, & \varphi_8 & \varphi_{11} & \varphi_{13}, & \varphi_{14} \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel & \shortparallel \\ id & \alpha & \alpha^2 & \alpha\gamma & \alpha^3 & \gamma & \alpha^3\gamma & \alpha^2\gamma \end{array}$$

C_8 ✗

$C_4 \times C_2$ ✓

$C_2 \times C_2 \times C_2$ ✗

D_8 ✗

Q_8 ✗

$(\alpha\gamma)(x) = \alpha(x^{11}) = x^{22} = x^7$

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

$(\alpha^2\gamma)(x) = \alpha^2 x^{11} = x^{44} = \varphi_{14} = \gamma\alpha^2$

почему мы так в этом уверенно

$\alpha^3\gamma(x) = \alpha^3(x^{11}) = x^{88} = \varphi_{13} = \gamma\alpha^3$

$Aut(C_{15}) = \{1, \alpha, \alpha^2, \alpha^3, \gamma, \alpha\gamma, \alpha^2\gamma, \alpha^3\gamma\}$ $\alpha^4 = 1$ $\gamma\alpha = \alpha\gamma$

$\gamma^2 = 1$

We showed $Aut(C_{15}) \cong \underset{\alpha}{C_4} \times \underset{\gamma}{C_2}$

Spec. Def-n

$C_4 = \{1, a, a^2, a^3\}$ $\quad a^4 = 1$ $\qquad C_2 = \{1, c\}$ $\quad c^2 = 1$

Formally

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

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

$AC = CA$ $\qquad (a,1)(1,c) = (a,c)$ $\qquad AC$

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

Beware standard confusion:

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

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

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

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

d/W 3 Revision of last year (not examinable)

Def-n Let 1) G be a group and
2) $H \subset G$

Say that H is a **subgroup** of G, when

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

equivalently when

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

Lagrange theorem

Lagrange's Theorem

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

Proof I

Def-n Let 1) G be a group and
2) $H \subset G$ a subgroup

If $x \in G$ $xH = \{xh : h \in H\}$ left coset of H by x
$Hx = \{hx : h \in H\}$ Right coset

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

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

Left cosets

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

Right cosets

$H \cdot 1 = \{1, y\} = H$
$Hx = \{x, yx\} = \{x, x^2y\}$
$Hx^2 = \{x^2, yx^2\} = \{x^2, xy\} =$
$Hy = \{y, 1\} = H$
$Hxy = \{xy, x^2\} = Hx^2$
$Hx^2y = \{x^2y, y\} = Hx$

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

25.01.11

II **Prop**

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

Proof:

Put $\lambda : H \to xH \quad \lambda(h) = xh$

λ injective $\quad \lambda(h_1) = \lambda(h_2)$

$$xh_1 = xh_2$$
$$x^{-1}xh_1 = x^{-1}xh_2$$
$$h_1 = h_2$$

λ is surjective by def^n of xH QED.

III Corollary $\boxed{\forall x \in G \quad |xH| = |H|}$

Example $G = D_3 = \{1, x, x^2, y, xy, x^2y\}$
$H = \{1, y\}$

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

Observe distinct cosets are disjoint
True in general

IV Prop.

Let $a, b \in G$

Then either $aH = bH$
or $aH \cap bH = \emptyset$

Proof

__need to proof__: $aH = bH \iff aH \cap bH \neq \emptyset$

($\Rightarrow$) $aH = bH \Rightarrow aH \cap bH \neq \emptyset$ (by logic)

__So__:

It suffices to show that if $(aH \cap bH) \neq \emptyset$ then $aH = bH$

So suppose $z \in (aH) \cap (bH)$

so $z = ah_1$ for some $h_1 \in H$

$z = bh_2$ for some $h_2 \in H$

so $ah_1 = bh_2$

$b^{-1}a = h_2 h_1^{-1} \in H$

$a = bb^{-1}a = bh_2h_1^{-1} \in bH$

so for each $\eta \in H$

$a\eta = bh_2h_1^{-1}\eta \in bH$

i.e. if $(aH) \cap (bH) \neq \emptyset$

then $aH \subset bH$

~~So by~~

Repeat the argument using the fact $(bH) \cap (aH) \neq 0$

to get $bH \subset aH$

So if $(aH \cap bH) \neq \emptyset$

□ then $aH = bH$ Q.E.D

__Main Pr__: **corollary** Lagrange's Thm

If 1) G is a finite group and

2) $H \subset G$ is a subgroup

Then $|H|$ div. $|G|$ exactly

__Proof__: list ~~different~~ the distinct cosets $x_1, \ldots, x_m$

Each X_i has the form

$X_i = x_i H$ for some $x_i \in G$

<u>claim</u>: $G = \bigcup_{r=1}^{m} X_i$

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

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

But distinct cosets are disjoint

i.e. $X_i \cap X_j = \phi$ $i \neq j$

so $|G| = |X_1| + |X_2| + \dots + |X_m|$

$|G| = |a_1 H| + |a_2 H| + \dots + |a_m H|$

But $|a_i H| = |H|$ for each i so

$|G| = m|H|$ QED

m = numb. of distinct cosets $\square$

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

$a_i H \cap a_j H = \phi$ if $i \neq j$

$\{a_1, \dots, a_m\}$ is then called a set of coset representatives.

There is no uniqueness about $\{a_1, \dots, a_n\}$

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

The distinct cosets are

$1 \cdot H, \; x \cdot H, \; x^2 H$

so $\{1, x, x^2\}$ is a set of coset rep-s for H on G

$$\begin{array}{ccc} yH & xy \cdot H & x^2 y H \\ \parallel & \parallel & \parallel \\ H & xH & x^2 H \end{array}$$

also list the distinct the cosets

So $\{y, xy, x^2y\}$ is also a set of coset rep-s

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

Q: When is $aH = bH$?

A: $aH = bH \iff b^{-1} a \in H$ Rule of equality of left cosets

Prop Rule of equality

$\boxed{aH = bH \iff b^{-1} a \in H}$

Proof: suppose $aH = bH$

For some $h_1, h_2 \in H$ $\; a h_1 = b h_2$

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

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

so $a = bh$ for some $h \in H$

so $a h' = b \underbrace{h h'}_{bH}$ for all $h' \in H$

so $aH \subset bH$

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

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

so by symmetry $bK \subset aK$

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

{Investigation : Semidirect Product} S1/W4 : 28.01.11

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

Contrast this with $C_3 \times C_2$

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

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

$$\begin{array}{cccccc} \| & \| & \| & \| & \| & \| \\ 1 & x & x^2 & y & xy & x^2y \end{array}$$

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

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

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

but is wrong!

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

{...} $C_3 \times C_2$ $x^3 = 1$ $y^2 = 1$ $yx = xy$

Semidirect Products

полупрямое произведение

Suppose G is a group $g \in G$

Consider $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$

Prop $\boxed{i_g \text{ is an automorphism of } G}$

Proof: 1) i_g is homomorphism:

$$i_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = i_g(x)\,i_g(y)$$

2) i_g is invertible with inverse $(i_g)^{-1} = i_{g^{-1}}$

$$\begin{aligned}(i_{g^{-1}} i_g)(x) &= i_{g^{-1}}(gxg^{-1}) \\ &= g^{-1}gxg^{-1}(g^{-1})^{-1} \\ &= (g^{-1}g)x(g^{-1}g) \\ &= x\end{aligned}$$

$i_{g^{-1}} i_g = Id \qquad i_g i_{g^{-1}} = id \qquad$ Q.E.D

Look at the assignment

$$g \mapsto i_g$$
$$i : G \longrightarrow Aut(G)$$

Prop: $\boxed{i : G \to Aut\, G \text{ is a homomorphism}}$

Proof: $i_{gh}(x) = gh(x)(gh)^{-1}$
and $(gh)^{-1} = h^{-1}g^{-1}$

So $i_{gh}(x) = g(hxh^{-1})g^{-1} = i_g(hxh^{-1}) = i_g(i_h(x)) = i_g i_h(x)$

{Note Mult in $Aut\, G$ is by composition}

True for all x so $i_{gh} = i_g \circ i_h \qquad$ Q.E.D

{...} Go back and look at D_6

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

Take $K = \{1, x, x^2\}$ subg-p of D_6

$Q = \{1, y\}$ — " — D_6

Look at homomorphism

$i : Q \to Aut(D_6)$

$i_{id}(g) = 1g1^{-1} = id$ $\quad i_1 = 1$

$i_y(g) = ygy^{-1}$, where $g \in G$

$i_y(1) = y1y^{-1} = 1$

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

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

Notice in this case: i_y defines an automorphism of K

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

$Q = \{1, y\}$

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

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

I want $yx = x^2y$ to get D_6

what do I need to do?

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

$= (i_y(x), y)$

1) Создаются и упоминаются во всех отделах!

2) потому что они связаны = будем их всё работать

φ: why there not more groups than homomorphisms?

Semidirect products:

1) Three ingredients:

1) a group K
2) a group Q
3) a homomorphism
$\varphi : Q \to \mathrm{Aut}(K)$ (operator homomorphism)

2) New multiplication Rule

$$* : (K \times Q) \times (K \times Q) \longrightarrow K \times Q$$

$$(k_1, q_1) * (k_2, q_2) = (k_1\, \varphi(q_1)(k_2),\ q_1 q_2)$$

H/W: Have to check this gives a group (Exercise)

Four cases: $(k_1, 1) * (k_2, 1) = (k_1\, \varphi(1)(k_2), 1 \cdot 1)$

$\varphi : Q \to \mathrm{Aut}(K) \qquad \varphi(1)(k_2) = k_2 \qquad \varphi(1) = Id$

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

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

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

IV CRUCIAL CASE:
$(1, q_1) * (k, 1) = (1\, \varphi(q_1)(k), q_1 \cdot 1) = (\varphi(q_1)(k), q_1)$

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

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

D_6 compared with $C_3 \times C_2$:

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

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

Final ingridient is a homomorphism

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

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

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

как мы утверждали

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

что это homomorphism

A: TWO:

1) $h(y) = 1$ $\qquad$ Trivial

2) $h(y) = \tau$ $\qquad$ non-Trivial

$\Rightarrow$

Calculate product in non-Trivial case

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

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

I've got D_6

whereas in trivial case

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

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

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

Def-n. 'Formal'

Let K be a group
Q be a group
$h : Q \to Aut(K)$ a homomorphism

Then the **semidirect product**
$K \rtimes_h Q$
is obtained as follows
1) Underlying set is $K \times Q$
2) multiplication $* \quad (K \times Q) \times (K \times Q) \to K \times Q$ given by
$$(k_1, q_1) * (k_2, q_2) = (k_1 h(q_1)(k_2), q_1 q_2)$$

The nonabelian group of order 21, $G(21)$ — 1/02/11

$K \rtimes_h Q \qquad h : Q \to Aut(K)$

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

We need a homomorphism $h : C_3 \to Aut(C_7)$

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

φ_3 has order 6 → почему

$\varphi_3 = \varphi_3 \quad x \quad 6$
$\varphi_3^2 = \varphi_2 \quad x^2 \quad 3 \Leftarrow$
$\varphi_3^3 = \varphi_6 \quad x^3 \quad 2$
$\varphi_3^4 = \varphi_4 \quad x^4 \quad 3 \leftarrow$
$\varphi_3^5 = \varphi_5 \quad x^5 \quad 6$
$\varphi_3^6 = Id \quad x^6 \quad 1 \leftarrow$

41
27
×27
189
54
729

$\varphi_3(x) = x^3$

$\varphi_3^2(x) = \varphi_3 \circ (\varphi_3(x)) = \varphi_3(x^3) = x^9 = x^2$
$\cong ?$
$\varphi_3(x^2) = \varphi(x)\varphi(x) = x^3 \cdot x^3 = x^6$

$\varphi_3^3(x) = \varphi_3 \circ (\varphi_3^2(x)) = x^{27} = x^6 = \varphi_6$
$\varphi_3(x^3) = \varphi_3(x)\varphi_3(x)\varphi_3(x) = x^9$

$\varphi_3^6(x) = (x^{27})^{27} = x^{729} = x^{29} = x = Id$

Must have ord $h(y)$ div. 3

Three possible homomorphisms:

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

2) 1^{st} non trivial choice $h(y) = \varphi_2$ $h(y) = \varphi_2(x) = x^2$
3) 2^{nd} non trivial choice $h(y) = \varphi_4$

1 with 1^{st} non-trivial choice
crucial calculation
$$(1, y) * (x, 1) = (h(y)(x), y)$$
so $(1, y) * (x, 1) = (x^2, y)$

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

so $X^7 = 1$ $Y^3 = 1$

crucial calculation : $YX = X^2Y$

So get a group of order 21 whose elements are

$$\left.\begin{matrix} \{1, X, X^2, X^3, X^4, X^5, X^6, \\ Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y \\ Y^2, XY^2, X^2Y^2, X^3Y^2, X^4Y^2, X^5Y^2, X^6Y^2\} \end{matrix}\right\} \text{Canonical}$$

The multiplication on this group is given by
$$X^7 = 1, \quad Y^3 = 1, \quad YX = X^2Y$$

② Next take the trivial choice

$h(y) = \mathrm{Id}$ $\qquad h(y)\, x = x$

Critical calculation becomes

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

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

So $yx = xy$ $\qquad \cong$

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

So trivial case gives Direct product

Prop. $\boxed{\text{Trivial choice always gives Direct Product}}$

③ Now let's take 2nd non trivial choice

$h(y) = \varphi_4 \qquad \varphi_4(x) = x^4$

Critical calc : $(1, y) * (x, 1) = (x^4, y)$

$yx = x^4 y \quad , x^7 = 1 \quad , y^3 = 1$

Conclusion:

- For each choice I get a group of order 21 whose elements have canonical form $x^a y^b$ $\begin{pmatrix} 0 \le a \le 6 \\ 0 \le b \le 2 \end{pmatrix}$

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

How many different groups?

At least 2 { one commutes
one doesn't

At most 3

In fact $(\mathrm{I}) \cong (\mathrm{II})$

start with 2nd non-triv. ch. again

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

$1 \to 1$

$y \to \varphi_4 \qquad (\varphi_4)^2 = \varphi_2$

$y^2 \to \varphi_2$

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

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

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

$1 \to 1$

$z \to \varphi_2$

$z^2 \to \varphi_4$

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

$zx = x^2 z$

$x^7 = 1 \quad z^3 = 1 \quad zx = x^2 z$

$(\mathrm{I}) \cong (\mathrm{III})$ by taking change of variables $y \to y^2$ in C_3 ($y^2 = z$)

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

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

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

Example $C_{11} \rtimes_h C_5$? $\quad C_5 \to Aut(C_{11})$

$\{1, y, \dots, y^4\}$

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

~~where $\alpha = \varphi_2$~~

orders $\quad 1, 10, 5, 10, 5, 2, 5, 10, 5, 10$

So get 5 homomorphisms

$h_0, \dots, h_4 : C_5 \to Aut(C_{11})$

$h_0(y) = 1$

$h_1(y) = \varphi_4 \quad \to \quad yx = x^4 y$

$h_2(y) = \quad \vdots$

H/WS: 04/02/11

H/WS Most groups of "small order" are semidirect products ("small" = divisible by two primes a small numb. of times:

e.g. 17×43 small, 16 big)

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

Recognition criterion

Def-n Normal subgroups

Suppose K is a subgroup of G

Say that K is **normal** in G

when $\forall x \in G \quad xK = Kx$

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

French: "distingué"

example 1) $G = D_6 \qquad K = \{1, x, x^2\}$

K is normal in D_6, as
$xK = Kx$
as $K = xK = x^2K$
$\quad K = Kx = Kx^2$ || so $xK = Kx$
$\qquad\qquad\qquad x^2K = Kx^2$

$yK = \{y, yx, yx^2\} = Ky \qquad yK = Ky$
$\quad = \{y, x^2y, xy\} \qquad xyK = Kxy$
$\qquad\qquad\qquad\qquad x^2yK = Kx^2y \quad \Rightarrow$ QED

whereas in D_6 if $H = \{1, y\}$
$xH = \{x, xy\} \qquad Hx = \{x, x^2y\}$
$xH \neq Hx$ so H not normal

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

Thm Recognition Criterion:

Let G be a finite group
Suppose G has subgroups K, Q, s.t.
i) $K \triangleleft G$
ii) $|G| = |K||Q|$
iii) $K \cap Q = \{1\}$
Then $G \cong K \rtimes_\phi Q$ for some homomorphism $\phi : Q \to \mathrm{Aut}(K)$

e.g. in $D_6 = G$

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

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

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

so $D_6 \cong K \rtimes_h Q \quad (= C_3 \rtimes_h C_2)$

Proof of Recogn. Criterion

Suppose given G, K, Q as above

Let $q \in Q$, $k \in K$

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

$(qkq^{-1} \in K)$

$(qK = Kq)$

Define $h: Q \to \mathrm{Aut}(K)$ by

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

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

$$h(q)(k_1 k_2) = q k_1 k_2 q^{-1} = (q k_1 q^{-1})(q k_2 q^{-1}) = h(q)(k_1)\, h(q)(k_2)$$

$h_q(a) = q a q^{-1}$

$h_q(k_1 k_2) = h_q(k_1) h_q(k_2)$

QED

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

2) h is itself a homomorphism:

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

so $h(q_1 q_2) = h(q_1) \circ h(q_2)$

claim: that $G \cong K \rtimes_h Q$ $(= K \times Q$ wrt multiplication by $h)$

$(\Leftarrow)$

Define $\Phi : K \rtimes_h Q \to G$ by

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

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

1) Φ is a homomorphism:

$$\Phi\left((k_1, q_1) * (k_2, q_2)\right) = \Phi\left(k_1 h(q_1)(k_2),\ q_1 q_2\right) = k_1 h(q_1)(k_2) q_1 q_2 =$$
$$= k_1 (q_1 k_2 q_1^{-1}) q_1 q_2 = k_1 q_1 k_2 q_2 = \Phi(k_1, q_1)\Phi(k_2, q_2)$$

So Φ is a homomorphism. as claimed

2) Φ is injective:

Suppose $\Phi(k, q) = \Phi(k', q')$

$$\therefore\ k q = k' q'$$
$$(k')^{-1} k = q' q^{-1}$$

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

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

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

similarly $q = q'$.

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

i.e. Φ injective

$|K \times Q|$

$\shortparallel$ by hypothesis

But $|K \rtimes_h Q| = |K||Q| = |G|$

$\Phi : K \rtimes_h Q \to G$ injective both finite sets same size $\Rightarrow$ Φ is surjective QED.

classification of groups:

obvious statement:

Thm $\boxed{\text{If } p \text{ is prime and } |G| = p \text{ then } G \cong C_p}$

Proof

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

ord(x) div. $|G|$ ord$(x) \neq 1$

So ord$(x) = p$

and (by listing):

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

So $G \cong C_p$ ∎

We'll show

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

Proof Let $|G| = 2p$

Suppose I know (by some method or other)

that (1) G has an element x of order p (ord$x = p$)

(2) G ... " —— y — " — 2 (ord$y = 2$)

If I knew this, then

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

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

Proof:

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

$Q = \{1, y\} \cong C_2$ $(\operatorname{ord} y = 2)$ → как я ∉ убеди что они не будут равны

почему группа (ord)

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

$y \notin K$ as $\operatorname{ord}(y) = 2 \nmid p$ (not div)

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

Also K is normal in G

G/K

$G/K = \{K, yK\}$ .. $G = K \cup yK$ $K \cap yK = \emptyset$

$K \backslash G = \{K, Ky\}$ $G = K \cup Ky$ $K \cap Ky = \emptyset$ $\Bigg\} \Rightarrow$

$\Rightarrow$ so ~~~~ $yK = Ky$

so $x^a y^b K = K x^a y^b$ $(\forall a, b)$

i.e. K is normal.

So conditions for Recognition Criterion hold

So $G \cong K \rtimes_h Q$
$\cong C_p \rtimes_h C_2$ for some h ■

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

1) G has an element of order p

2) G has element of order 2
3) Describe all homomorphisms $h: C_2 \to Aut(C_F)$

First show

Theorem

Let G be a finite group

suppose that $\forall g \in G$, $g^2 = 1$

then $G \cong \underbrace{C_2 \times C_2 \times \dots \times C_2}_{n}$

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

Proof:

G is necessary abelian:

let $x, y \in G$ $\quad x^2 = 1 \quad y^2 = 1 \quad \Big| \; x^{-1} = x, \; y^{-1} = y$

also $(xy)^2 = 1$

$xyxy = 1$

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

$y^{-1}x^{-1} = xy$ $\quad \Rightarrow yx = xy$ for all x, y

cheat rewrite G additively:

1 becomes 0

$x^2 = 1 \;\dots\to\; 2x = 0$

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

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

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

Rewrite multiplicatively again

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

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

$0 \longrightarrow 1$

$1 \longrightarrow x$

Q.E.D

08/02/11

We showed that if G satisfies $x^2 = 1$ for all $x \in G$ then $|G| = 2^n$ $(G \cong \underbrace{C_2 \times C_2 \times \dots \times C_2}_{n})$

Let p be odd prime and

$|G| = 2p$

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

Let $x \in G$

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

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

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

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

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

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

So either

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

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

Prop. Let p be an odd prime, and g group $|g| = 2p$

Then a) $\exists\, x \in g$ ord $x = p$
b) $\exists\, y \in g$ ord $y = 2$

Proof:
suppose (i) above holds,
let $z \in g$ have ord $(z) = 2p$

Then take $x = z^2$ ord $x = p$
& take $y = z^p$ ord $y = 2$

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

So suppose ii) above holds &
let $x \in g$: ord$(x) = p$

how do we prove that K is a subgroup (a real group?)

why it is a subgroup?

Then $K = \{1, x, \dots, x^{p-1}\}$ K is a subgroup of g

Consider $g/K = |g/K| = |g|/|K| = 2p/p = 2$ → why this true?

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

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

As $w^2 \in K$ either
$w^2 = 1$ or $w^2 = x^a$ $(1 \le a \le p-1)$

If $w^2 = 1$ put $y = w$ $\Rightarrow$ $ord(y) = 2$

If $w^2 \neq 1$ then $ord(w^2) = p$ very disagree

So $ord(w) = 2p$ and put $y = w^p$ $\Rightarrow$ $ord(y) = 2$

The exhausts all possibilities

In any case $\exists\, x \in G$ $ord(x) = p$
$\exists\, y \in G$ $ord(y) = 2$ ■

{the story so far...
$|G| = 2p$ $\exists\, x \in G$ $ord(x) = p$
$\exists\, y \in G$ $ord(y) = 2$
Now read on {

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

Proof: (already in details proved by parts: loose previous thm)
extra work: Put $K = \{1, x, \dots, x^{p-1}\}$ $x^p = 1$ $ord(x) = p$
$Q = \{1, y\}$ $y^2 = 1$ $ord(y) = 2$

$K \cong C_p$ $Q \cong C_2$
Claim that $K \lhd Q$ why?

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

$G = K \cup Ky$ so $yK = Ky$ (only 2 cosets)

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

so $x^a y^b K = K x^a y^b \quad 0 \le a \le p-1$

so $K \lhd G$ as claimed $\quad 0 \le b \le 1$

Now apply Recognition Criterion

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

So $G \cong K \rtimes_h Q$

$\cong C_p \rtimes_h C_2$ for some $h : C_2 \to Aut(C_p)$ ∎

How many homomorphisms $h : C_2 \to Aut(C_p)$?

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

Proof: Let $C_p = \{1, x, \dots, x^{p-1}\}$ & consider $x\alpha(x) \in C_p$

Either (a) $x\alpha(x) = 1$

or (b) $x\alpha(x) \neq 1$

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

(b) then $x\alpha(x)$ generates C_p i.e.

as $x\alpha(x) \neq 1$ & $\in C_p$ & $\forall g \in C_p$ ord$(g) \mid p$ ord$(g) = 1$ or $= p$ $\Rightarrow o(x\alpha(x)) = p$

but $\alpha(x\alpha(x)) = \alpha(x)\alpha^2(x)$

$= \alpha(x)\, x$

$= x\alpha(x)$ (C_p abelian)

& α takes a generator to itself, so $\alpha = id$ ∎

Corollary: If p is an odd prime & $|G| = 2p$

Then either $G \cong C_{2p}$ $(\cong C_p \times C_2)$
or $G \cong D_{2p}$

Proof: With $G \cong C_p \rtimes_h C_2$
where $h: C_2 \to Aut(C_p)$

Let $C_p = \{1, x, \ldots, x^{p-1}\}$ & $C_2 = \{1, y\}$

look at $h(y) \in Aut(C_p)$ (& h is homomorphism)

clearly $h(y)^2 = Id$ $(= h(y^2))$

So either $h(y) = id$ & $G \cong C_p \times C_2 \cong C_{2p}$
or $h(y)(x) = x^{-1}$ & $G \cong D_{2p}$ ∎

how far have we got?

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

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

11/02/11

Last lecture:

p odd prime

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

If $p = 2$ $2p = 4$

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

Proof:

If $\exists x \in G$ почему они все будут разными? упр 1

$ord(x) = 4$ then $G \cong C_4$

the alternative

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

We need to show:

(i) G has an element of order p

(ii) G " p^2

We come to

thm **Sylow's Theorem** (= 'seal off')

$\boxed{\begin{array}{l} \text{Let } p \text{ be a prime} \\ G \text{ be a finite group s.t. } |G| = k\,p^n, \\ \quad \text{where } k \text{ is coprime to } p \\ \\ \text{then (i) } G \text{ has a subgroup of order } p^n \\ \quad \text{(ii) if } N_p = \text{numb. of subgroup of order } p^n \\ \quad\quad \text{then } N_p \equiv 1 \pmod p \\ \quad \text{(iii) } N_p \text{ div } |G| \\ \quad \text{(iv) If } H \text{ is a subgroup of order } p^m \ (m \leq n), \\ \quad\quad \text{and } K \text{ is a subgroup of order } p^n, \\ \quad\quad \text{then } \exists x \in G \quad xHx^{-1} \subset K \end{array}}$

Example of "Sylow counting"

we show that if $|G| = 21$

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

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

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

trick: go for the biggest prime first

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

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

N_7 = the numb of such subgroup

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

Claim that, in fact, $N_7 = 1$

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

Otherwise suppose $N_7 \geq 8$
let $K_1, \dots, K_8$ each be a subgroup of order 7

Each K_i has six elements of order 7

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

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

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

However $|G| = 21 < 48$

Contradiction.
Hence $N_7 = 1 \Rightarrow K$ is unique

[So let K be the unique subgroup of order 7
If $x \in G$ xKx^{-1} is also a subgroup of order 7

why? it could be a coset

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

so $K \triangleleft G$

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

$Q \cong C_3$

As 7 and ~~...~~ 3 are coprime, then

$K \cap Q = \{e\}$

So now apply Recogn. Criterion to conclude that

$G \cong K \rtimes_h Q$

$\cong C_7 \rtimes_h C_3$ for some h

Two lectures ago showed, that therefore

$G \cong C_7 \times C_3$

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

Q.E.D.

n	G with $\lvert G \rvert = n$	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	✓

n	G with $\|G\| = n$	complete
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_8, Q_8$	?
9	$C_9, C_3 \times C_3$	?
10	C_{10} D_{10}	V
11	C_{11}	V
12	$C_{12}, C_2 \times C_6, D_{12}, A_4, D_6^*$	?
13	C_{13}	V
14	C_{14}, D_{14}	V
15	$C_{15} = C_5 \times C_3$	
16	REAL MESS	
17	C_{17}	V
18	A BIT OF A MESS	
19	C_{19}	V
20		
21	C_{21}, $G(21)$	V
22	C_{22}, C_{2}	V
23	C_{23}	V
24	DO ABLE	
25	C_{25}, $C_5 \times C_5$	
26	C_{26}, D_{26}	V
27	REAL MESS	
28	EVEN APPEARED IN EXAM	
29	C_{29}	V

Def^n Binary dihedral groups:

D^*_{2n} has order $4n$

$D^*_{2n} = \langle xy \mid x^n = 1, y^{n \pm 1} = 1, yx = x^{n-1} y \rangle$

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

Prop. $\boxed{\text{Let } G \text{ be a group with } |G| = 15 \text{ then } G \cong C_{15} \cong C_5 \times C_3}$

Proof (by Sylow counting)

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

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

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

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

contradiction. So $N_5 = 1$

So K is unique subgroup of order 5

~~so~~ N

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

so $xKx^{-1} = K$ $\quad K \trianglelefteq G$

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

so $G \cong K \rtimes_h Q \cong C_5 \rtimes_h C_3$

How many possibilities for h

$h : C_3 \to Aut(C_5) \cong C_4$

h must be

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

Group actions and the class equation

22/01/11

Def^n Let $\mathcal{G}$ be a group
X be a set

By (left) **action of $\mathcal{G}$ on X** we mean a mapping
$\circ : \mathcal{G} \times X \to X$

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

s.t. 1) $(gh) \circ x = g \circ (h \circ x)$ $\quad g, h \in \mathcal{G}, x \in X$

2) $1 \circ x = x$ $\quad x \in X$

Examples: 1) Left translation

$X = \mathcal{G}$, $\circ$ = group multiplication

$\mathcal{G} \times \mathcal{G} \to \mathcal{G}$
$g \circ x \equiv gx$

2) Right translation

Again $X = \mathcal{G}$
$\mathcal{G} \times X \to X$
$g \circ x = x g^{-1}$

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

3) Conjugation (Interesting example)

Again $X = \mathcal{G}$, but
$* : \mathcal{G} \times X \to X$ $\quad g * x = g x g^{-1}$
Combines both left and right translation

Def-n. Orbit of an element

Let $\cdot : G \times X \to X$ be an action

$x \in X$

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

Example

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

$G \times X \to X$

$g \circ z = g z g^{-1}$

Let's compute the orbits!!

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

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

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

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

2) $\langle x \rangle = \{ g x g^{-1} : g \in D_6 \} = \{ 1x1^{-1}, x x x^{-1}, x^2 x x^{-2}, y x y^{-1}, (xy) x (xy)^{-1}, (x^2 y) x (x^2 y)^{-1} \} =$

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

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

3) $\langle x^2 \rangle = \{ 1 x^2 1^{-1}, x x^2 x^{-1}, x^2 x^2 x^{-2}, y x^2 y^{-1}, (xy) x^2 (xy)^{-1}, (x^2 y) x^2 (x^2 y)^{-1} \}$

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

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

4) $\langle y \rangle = \{ 1y1^{-1}, xyx^{-1}, x^2yx^{-2}, yyy^{-1}, \cancel{xy}y(xy)^{-1}, (x^2y)y(x^2y)^{-1} \} =$
$= \{ y, x^2y, xy, y, x^2y, xy \}$

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

i.e. $\langle y \rangle = \{ y, xy, x^2y \}$

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

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

To summarise:

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

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

$\langle y \rangle = \{ y, xy, x^2y \}$ $(= \langle xy \rangle = \langle x^2y \rangle)$

So three orbits $\langle 1 \rangle, \langle x \rangle, \langle y \rangle$

Notice (again) distinct orbits have empty intersection.

e.g. $\langle 1 \rangle \cap \langle x \rangle = \phi$

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

$\langle x \rangle \cap \langle y \rangle = \phi$

~~The class~~

The class equation for this action:

$X = \langle 1 \rangle \cup \langle x \rangle \cup \langle y \rangle$ - set theoretic version

Numerical version of class equation

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

$6 = 1 + 2 + 3$

In general

Given $\circ : G \times X \to X$ action

Prop. Let $x, y \in X$

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

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

(In English, distinct orbits are disjoint)

Proof:

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

enough to prove

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

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

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

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

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

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

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

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

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

Let $\gamma \in G$ $\gamma \circ x = (\gamma g^{-1} h) \circ y$

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

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

For all $\gamma \in G$ $\gamma \circ y = (\gamma h^{-1} g) \circ x$

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

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

so $\langle x \rangle = \langle y \rangle$ QED

25/02/11

Notice if $x \in X$ $x \in \langle x \rangle$

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

Def-n Let $x_1, \dots, x_m \in X$ be such that $\langle x_i \rangle \neq \langle x_j \rangle$ if $i \neq j$ and such that for each $x \in X$

$\exists i$ $x \in \langle x_i \rangle$

i.e. $\langle x_1 \rangle, \langle x_2 \rangle, \langle x_3 \rangle, \dots, \langle x_m \rangle$ lists all distinct orbits

⇒ set theoretic class eq-n (0 version)

$$X = \bigsqcup_{i=1}^{m} \langle x_i \rangle$$ Disjoint union

Numerical form (1st version)

$$|X| = \sum_{i=1}^{m} |\langle x_i \rangle|$$

Example: let $X = G = D_6$, acting on itself by conjugation
The orbits are

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

One choice of orbit reps

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

So we this choice

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

Choice not unique in general. Could also take

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

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

Numerical class eq-n here is
$6 = 1 + 2 + 3$
(no double counting. Different orbits are disjoint)

Def-n More useful form of class Eq-n

$\cdot : G \times X \to X$ action

Let $x \in X$.

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

Prop G_x is a subgroup of G

Proof:

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

2) $g, h \in G_x$ then
$$(gh) \cdot x = g \cdot (h \cdot x) \underset{h \in G_x}{=} g \cdot x \underset{g \in G_x}{=} x$$

so $gh \in G_x$.

3) If $g \in G_x$
$$x = 1 \cdot x = (g^{-1} g) \circ x = g^{-1} \circ (g \circ x) = g^{-1} \cdot x$$

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

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

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

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

$1x1^{-1} = x$ $\quad 1 \in G_x$ $\quad yxy^{-1} = x^2yy^{-1} = x^2$

$xxx^{-1} = x$ $\quad x \in G_x$ $\quad y \notin G_x$

$x^2xx^{-2} = x$ $\quad x^2 \in G_x$ $\quad xy \notin G_x, \; x^2y \notin G_x$

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

G_y ?? $\quad 1 \in G_y$

$yyy^{-1} = y$ $\quad y \in G_y$

$xyx^{-1} = x^2y \neq y$ $\quad x \notin G_y$

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

H/W check

$G_1 = D_6$

$G_x = \{1, x, x^2\} = G_{x^2}$

$G_y = \{1, y\}$

$G_{xy} = \{1, xy\}$

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

Prop Let $\cdot : G \times X \to X$ be an action. Let $z \in X$, then there is a bijection

$$G/G_z \longleftrightarrow \langle z \rangle$$

Proof

The elements of G/G_z are subsets of G of the form

$$g \cdot G_z = \{ga : a \in G_z\}$$

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

Define a mapping $\phi : G/G_z \to \langle z \rangle$ by $\phi(g \cdot G_z) = g \circ z$

Ψ is well defined:

Suppose $g \cdot G_z = h \cdot G_z$, then

$h^{-1}g \in G_z$ so $(h^{-1}g) \cdot z = z$

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

$g \cdot z = h \cdot z$

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

Ψ obviously surjective by def-n of $\langle z \rangle$ почему сюръективно по опред?

Go to show Ψ is injective

вот верни по другому

Suppose $\Psi(g \cdot G_z) = \Psi(h \cdot G_z)$

so $g \cdot z = h \cdot z$

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

so $h^{-1}g \in G_z$ so $g \cdot G_z = h \cdot G_z$

i.e. Ψ is injective

hence bijective QED

why $|G/G_z| = |G|/|G_z|$

Corollary $\boxed{|\langle z \rangle| = |G|/|G_z|}$

check with the action of D_6 on itself by conjugation

Three orbits $\langle 1 \rangle, \langle x \rangle, \langle y \rangle$

$\langle 1 \rangle = \{1\}$ $\quad |\langle 1 \rangle| = |D_6|/|G_1| = 6/6$

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

$G_x = \{1, x, x^2\}$ $\quad |G_x| = 3$

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

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

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

Really useful version of Class Eq-n

Prop. Let $\cdot : G \times X \to X$ action $\begin{cases} G \text{ finite} \\ X \text{ finite} \end{cases}$

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

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

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

& $|\langle x_i \rangle| = |G| / |G_{x_i}|$ so substitute back

Q.E.D.

Def-n Fixed Point set of an action

Let $\cdot : G \times X \to X$ be an action

Define $X^G = \{x \in X : \forall g \in G \ g \cdot x = x\}$

X^G is the **fixed point set**

Another way of saying this is that

$\to$ $x \in X^G \iff \langle x \rangle = \{x\}$

Prop. 1st Real application of ~~eq~~ class eq-n:

Let p be a prime
G be a group $|G| = p^n$
acting on a finite set X

then $|X| \equiv |X^G| \pmod{p}$

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

choose them in such a way that fixed points come first
i.e. $X^G = \{x_1, \ldots, x_k\}$ $k \le m$

if there is no ~~set~~ fixed point in a set.

and $x_i \notin X^G$ $k < i$

$\langle x_r \rangle = \{x_r\}$ for $1 \le r \le k$
$|\langle x_r \rangle| = 1$ for $1 \le r \le k$

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

Write down the class eq-n

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

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

$|G| = p^n \Rightarrow |G_{x_i}| = p^{m_i}$ $m_i \le n$
and since $|G_{x_i}| \neq |G|$ $k < i$
Then $p^{m_i} < p^n$ $k < i$

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

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

$|X| = k \mod p \quad |X| \equiv |X^g| \mod p$

$\therefore k = |X^g|$ **Q.E.D**

01/03/11

Application of Class Eq-n

Thm Wilson's Theorem.

Let. p be a prime
$1 \le k$ be an integer $(k \in \mathbb{N})$

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

Proof:

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

consider the action

$\cdot : G \times X \to X$

$g \cdot (h, i) = (gh, i) \quad h \in G, \ i \in \{1, \ldots k\}$

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

Q: How big is $\mathcal{X}$?

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

$\mathcal{G}$ also acts on $\mathcal{X}$ as follows:
Let $\mathcal{G} \times \mathcal{X} \to \mathcal{X}$, $(g, A) \to g \cdot A$
be the action $g \cdot A = \{ga : a \in A\}$, where $A \in \mathcal{X}$

To prove Wilson's thm enough to show $|\mathcal{X}^{\mathcal{G}}| = k$

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

$|\mathcal{X}| = |\mathcal{X}^{\mathcal{G}}| \mod p$

$1 \to 1$
$s \to t$
$t \to st$
$st \to s$

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

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

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

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

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

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

So $\mathcal{X}^{\mathcal{G}} = \{\mathcal{G} \times \{1\}, \mathcal{G} \times \{2\}, \ldots, \mathcal{G} \times \{k\}\} \Rightarrow |\mathcal{X}^{\mathcal{G}}| = k$

Q.E.D.

Theorem Sylow Part I

Let p be a prime
$k \geq 1$ be coprime to p
G be a group $|G| = kp^n$

then $\exists$ subgroup H of G : $|H| = p^n$

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

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

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

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

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

Let G act on $\mathcal{P}$ by

$$G \times \mathcal{P} \to \mathcal{P}$$

$$g.A = \{ga : a \in A\}$$

mult. in G

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

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

Let $A_1, \ldots, A_m$ be a set of orbit reps in $\mathcal{P}$ for the above action

Let $\mathcal{G}_2 = \mathcal{G}_{A_i} = \{ g \in \mathcal{G} : gA_i = A_i \}$

The class eq-n now gives

$$|\mathcal{G}| = |\mathcal{G}|/|\mathcal{G}_1| + \dots + |\mathcal{G}|/|\mathcal{G}_m| = \sum_{i=1}^{m} |\mathcal{G}|/_{\mathcal{G}_i} \quad (m > 1)$$

$|\mathcal{G}| = kp^n \qquad |\mathcal{G}_i| = k_i p^{e_i} \qquad e_i \leq n$

and $k_i < k$

(k_i div k)

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

By Wilson's Thm

$$k \equiv \sum_{i=1}^{m} p^{n-e_i} \quad (\text{mod } p)$$

If each $e_i < n$ then

RHS $\equiv 0$ mod p

LHS $\equiv k \neq 0$ mod p

<u>Contradiction</u>

so for some i $e_i = n$

$|\mathcal{G}_i| = k_i p^n \qquad k_i < k$

Now appeal to Induction Hypothesis

$\mathcal{G}_i$ is a group of order $k_i p^n$ $k_i < k$

so $\mathcal{G}_i$ has a subgroup H

$|H| = p^n$

$H \subset \mathcal{G}_i \subset \mathcal{G}$

So H is a subgroup of G

$|H| = p^n$

Q.E.D.

Theorem Sylow Part II

Let p be a prime

$k \geq 1$ is a coprime to p

G be a group $|G| = kp^n$

Put N_p = no of subgroups of order p^n

Then $N_p \equiv 1 \pmod p$

Proof

Let S denote the set

$S = \{Q \subseteq G : |Q| = p^n$ and Q is a subgroup$\}$

$S \neq \emptyset$ by Sylow Part I

$|S| = N_p$ (def-n of N_p)

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

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

Consider the following action of P on S

$P \times S \to S$

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

Since $|P| = p^n$ then

$|S| \equiv |S^P| \pmod p$

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

$N_p \equiv |S^P| \pmod p$ by def-n

To complete the proof we must show there is only one fixed point under the action i.e. $|S^P| = 1$

~~Note~~ Then $N_p \equiv 1 \mod p$

4/03/11

clearly $P \in S^P$

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

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

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

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

I claim: PQ is a subgroup of G

$1 = 1 \cdot 1 \in PQ$

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

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

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

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

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

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

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

QED (PQ is a subgroup)

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

Consider PQ/Q. How big it is?

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

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

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

(concentrate on rule of equality for cosets)

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

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

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

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

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

so $xQ = x'Q$ QED. well defined

ii) Injective:

suppose $\vartheta(x(P \cap Q)) = \vartheta(y(P \cap Q))$

$$xQ = yQ$$

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

so $y^{-1}x \in P \cap Q$ so $x(P \cap Q) = y(P \cap Q)$

QED. injectivity

iii) Surjective:

Let $pqQ \in PQ/Q$

$qQ = Q$

so $pqQ = pQ = \vartheta(p(P \cap Q))$

Q.E.D. surjectivity

conclusion: already known $|P/_{P \cap Q}| = |PQ/Q|$

$|P| = p^n$ so $|P/P \cap Q| = p^{n-l}$ where $|P \cap Q| = p^l$

so $|PQ/Q| = p^{n-l}$.

so $|PQ| = |Q| p^{n-l} = p^{2n-l}$

But PQ is a subgroup of G

$|PQ| = p^{2n-e}$ $\quad |G| = kp^n \quad p \not| k$

So $2n - e \le n$

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

$\therefore n \le 2n - e \le n$

$\therefore e = n$

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

$P \subset PQ \qquad |P| = |PQ|$

So $PQ = P$

$Q \subset PQ \quad |Q| = |PQ|$

so $PQ = Q$

so $P = Q$ & $S^P = \{P\}$

i.e. P is unique fixed point

$|S^P| = 1$

$\therefore N^P \equiv 1 \mod p$ $\qquad$ QED Fin.

9/W8

Ring Theory

Def-n 1) $\cdot : X \times X \to X$

$(x,y) \to x \cdot y$

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

X is a set

semi group

2) assume $\exists 1 \in X$ s.t. $1 \cdot x = x \cdot 1 = x$ — $\exists$ Identity

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

if add $\{\forall x \ \exists y : xy = 1 = yx$ **Inverses**$\} \Rightarrow$ it is a **group**

ex: Take $\mathbb{Z}$: Two operations

$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ — 0 identity, $-x$ inverse. Additive group

$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ — 1 identity, don't have inverses. multiplicative monoid.

both commutative

$x \cdot (y + z) = xy + x \cdot z$

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

1) R is a set $0, 1 \in R$

2) $+ : R \times R \to R$ commutative group operation with 0 = additive identity — $(R, +, 0)$ abelian group

3) $(R, \cdot, 1)$ is a multiplicative monoid

4) $x \cdot (y+z) = x \cdot y + x \cdot z$, $(y+z) \cdot x = y \cdot x + z \cdot x$ $\forall x,y,z \in R$

Distributive law

Note: We will consider only commutative rings

(i.e. $\forall x, y \in R \quad x \cdot y = y \cdot x$)

standard example: 1) $\mathbb{Z}$

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

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

A noncommutative example:

Let R be a ring (any ring!)

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

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

a more ring

Def-n Polynomial rings:

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

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

add & multiply in obvious way

More generally if R is a ring

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

ring of polynomials with coef-nts in R

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

Def-n $\boxed{\text{A field } \mathbb{F} \text{ is a ring in which } x \neq 0 \Rightarrow \exists x^{-1} \in \mathbb{F} : x x^{-1} = 1 \quad x^{-1} x = 1}$

e.g. 1) $\mathbb{Q}$ field

2) $\mathbb{F}_p$ field with p elements p prime

$\mathbb{F}_p = \{0, 1, \dots, p-1\}$ (Addition & multiplication p)

Comming soon!!! $\mathbb{F}_{p^2}$ field with p^2 elements

Quotient Rings → Понят.-кольцо

08/03/11

start with two examples:

i) $\mathbb{Z}$ ii) $\mathbb{F}[x]$ ring of polynomials in x with coef-nts in a field $\mathbb{F}$.

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

1) Dive any integer by n to get a remainder r $0 \le r \le n-1$

2) Add & multiply remainderes except we put $n \equiv 0$

Example 1) $\mathbb{Z}/3 = \{0, 1, 2\}$ $\mathbb{Z}/3$ is a field alternatively written $\mathbb{F}_3$

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

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

почему

↓

стр. 38½-3

10 лоуф не зачно

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

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

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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

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

We take possible remainders after dividing by x^2+x+1
Add & multiply but set:
$$\boxed{x^2 + x + 1 \equiv 0}$$

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

equivalently
$$x^2 = x + 1 \qquad (1 = -1 \text{ in } \mathbb{F}_2)$$

R/I {x+I : x∈R}

как это работает в поле ?!?

стр. 40 $\frac{1}{2}$

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

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

$\cdot$	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

0 in $\mathbb{F}_2$

$(x+1)(x+1) = x^2 + 2x + 1 = (x+1)+1 = x$ $\qquad$ $x^2 \equiv x+1$ (from above)

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

4) Contrast this with $\mathbb{F}_2[x]/x^2+1$

elements look the same $\{0, 1, x, x+1\}$

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	x
$x+1$	0	$x+1$	x	0

$x^2+1 \equiv 0$

$x^2 \equiv -1$

$x^2 \equiv 1$ over $\mathbb{F}_2$

<u>not</u> a field $x+1$ has no inverse

Def-n If R is a ring, the **unit group** R^* is the set of invertible elements under multiplication

$$\boxed{R^* = \{a \in R : \exists b \in R \ ab = 1 = ba\}}$$

R is a field $\iff R^* = R - \{0\}$

Example $\mathbb{F}_3[x]/x^2+1$ $\quad F_3=\{0,1,2\}$

Possible remainders:

$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$

$x^2+1\equiv 0 \iff x^2=-1 \iff x^2\equiv 2$

finish: rank?, remaining work

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	2						
$x+2$	0	$x+2$							
$2x$	0	$2x$							
$2x+1$	0	$2x+1$							
$2x+2$	0	$2x+2$							

Scheme Proof: $\mathbb{Z}/n \iff \mathbb{F}[x]/p(x)$ $\quad p(x)=x^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0$

(is a field, when n is prime) $\quad$ is a field iff is irreducible / $\mathbb{F}$

namely!

Def-n $p(x)=a_n x^n+\dots+a_1x+a_0$ is irreducible / $\mathbb{F}$, when there is no factorisation $p(x)=a(x)\,b(x)$

where $\deg(a)<n$ and $\deg b<n$

e.g. 1) x^2+x+1 is irred. / $\mathbb{F}_2$

2) $x^2+1=(x+1)^2$ is not irred / $\mathbb{F}_2$

3) However x^2+1 is irred / $\mathbb{F}_3$,

4) $\mathbb{R}[x]/x^2+1 \cong \mathbb{C}$ $\quad \Rightarrow x^2+1$ is irred / $\mathbb{R}[x]$

$\Rightarrow \mathbb{R}[x]/x^2+1$ is a field

why it is

11/03/11

A ring $R = (R, +, 0, \cdot, 1)$
consists of following data

i) $(R, +, 0)$ is an abelian group
$+ : R \times R \to R$ assoc., commute, $0 \in R$ identity
$\forall x \in R \ \exists -y \in R \quad x + (-y) = 0$

ii) $(R, \cdot, 1)$ monoid
$\cdot$ is assoc. (needn't be commut. in general)
1 identity

iii) $x \cdot (y+z) = xy + xz$
$(y+z) \cdot x = yx + z \cdot x$

Def-n If R, S are rings, by a **ring homomorphism**
$\varphi : R \to S$ we mean a mapping such that

$$\boxed{\begin{array}{ll} \text{(i)} \ \varphi(x+y) = \varphi(x) + \varphi(y) & \\ \text{(ii)} \ \varphi(xy) = \varphi(x)\varphi(y) & \forall x, y \in R \\ \text{(iii)} \ \varphi(1) = 1 & \end{array}}$$

why?

Automatically true that $\varphi(0) = 0$ from (i) & (ii)

Def-n $\varphi : R \to S$ is a **ring isomorphism** when
φ is a bijective homomorphism

Def-n $(R, +, 0, \cdot, 1)$ is a **subring** of $(S, +, 0, \cdot, 1)$ when

- $(R, +, 0)$ is a subgroup of $(S, +, 0)$
- $(R, \cdot, 1)$ is a submonoid of $(S, \cdot, 1)$

e.g. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a collection of subrings

Suppose N is a subgroup of G

$$G/N = \{xN : x \in G\}$$

G/N is a group when $N \trianglelefteq G$

N normal; otherwise [illegible] prop

$$G/N \times G/N \to G/N$$

$$(x \cdot N) \cdot (y \cdot N) = xy \cdot N$$

what does it mean W@:M

Question: Let R be a ring
suppose $I \subset R$ is a subset
what properties we need for I in order, that R/I is a ring (naturally)?

necessary?

$\boxed{\text{clearly need } I \text{ to be an additively subgroup of } R}$

So R/I is an additively group
what about mult. on R/I?

Def-n Let R be a ring (commutative)
$I \subset R$

Say that I is an **ideal** in R when

(i) I is an additive subgroup of R
(i.e) 1) $0 \in I$ 2) if $x, y \in I$, $x+y \in I$
3) if $x \in I$ then $-x \in I$

(ii) if $x \in I$ and $\lambda \in R$,
then $\lambda x \in I$
(so $x \lambda \in I$ ⇐ R commutative)

Prop Let I be an ideal in R
Then R/I has a ring structure, with property
that $q : R \to R/I$
$q(x) = x + I$ is a ring homomorphism

homomorphism

Observe: we write cosets additively $x + I$, because I is additive subgroup of R

Proof:
We need to define:
i) $+ : R/I \times R/I \to R/I$
ii) a 'zero-element in R/I'
iii) $\cdot : R/I \times R/I \to R/I$
iv) a 'unit element' $1 \in R/I$

(i) comes from the fact that I is normal as an additive subgroup

$$x + I = I + x$$

So we define: $(x+I) + (y+I) = (x+y) + I$

(ii) ~~Zero~~ the zero element is $0 + I \ (= I)$

iii) Define $(x+I) \cdot (y+I) = xy + I$

Need to check that $\cdot$ is well defined
i.e. answers is independent of way you've represent cosets.

$$x + I = x' + I \iff x - x' \in I$$

Suppose $\left.\begin{array}{l} x_1 + I = x_2 + I \\ \text{and } y_1 + I = y_2 + I \end{array}\right\}$
got to show $x_1 y_1 + I = x_2 y_2 + I$
(i.e got to show $x_1 y_1 - x_2 y_2 \in I$

$$x_1 y_1 - x_2 y_2 =$$

Trick: $x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2 =$
$= (x_1 - x_2) y_1 + x_2(y_1 - y_2)$ $\Big\Downarrow$ R commut.
$= y_1 (x_1 - x_2) + x_2(y_1 - y_2)$

$x_1 - x_2 \in I$ so $y_1(x_1 - x_2) \in I$ (I ideal)
$y_1 - y_2 \in I$ so $x_2(y_1 - y_2) \in I$

I is additive subgroup so

$$x_1 y_1 - x_2 y_2 = y_1(\underbrace{x_1 - x_2}_{\in I}) + x_2(\underbrace{y_1 - y_2}_{\in I}) \in I$$

so $x_1 y_1 + I = x_2 y_1 + I$
and multiplication is well define

(iv) Take $1 = 1 + I$ → Quotient ring

ϕ is tautologically a ring homomorphism

$$\phi(x+y) = (x+y) + I = (x+I) + (y+I) = \phi(x) + \phi(y)$$

$$\phi(x)\phi(y) = (x+I)(y+I) = xy + I = \phi(xy)$$

$$\phi(1) = 1 + I = 1$$

If I is an ideal in R then R/I is called the quotient ring of R mod I

Examples $\mathbb{Z}/n$

Take $R = \mathbb{Z}$
$I = \{\lambda n : \lambda \in \mathbb{Z}\}$ $(= (n))$

(n) is obviously ideal in $\mathbb{Z}$

Forming $\mathbb{Z}/n$, setting the ideal $(n) \equiv 0$
i.e. ideal (n) everytime you see n write 0)
Heuristic interpretation

WTF?

H/W 8 N1

~~[illegible]~~

можно

доказывать

Example: $\mathbb{F}[x]/p(x)$ (e.g. $p(x) = x^2 + x + 1$)

Here take $R = \mathbb{F}[x]$

$$I = \{ \lambda(x) p(x) ; \lambda(x) \in \mathbb{F}[x] \}$$

i.e. multiples of $p(x)$

Example: $\mathbb{F}_3 = \{0, 1, 2\}$ field with 3 elements

$$\mathbb{F}_3[x] / x^2+1 \cong \mathbb{F}_3[x] / \underset{\shortparallel}{x^2+2x+2} = \mathbb{F}_3[y] / y^2+2y+2$$

$\varphi(x) = y+1$

почему так можно? а не

$\varphi(x^2) = \varphi(x \cdot x) =$
$= \varphi(x) + \varphi(x)$

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

$\{1, x\}$ basis for $\mathbb{F}_3[x]/x^2+1$

$\{1, y\}$ ... $\mathbb{F}_3[y]/y^2+2y+2$

$$\varphi = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$1 \to 1 \qquad x \to 1+y$$

Need to check formally that

$$\varphi(a+bx)(c+dx) = \varphi(a+bx)\,\varphi(c+dx)$$

$$\varphi(a+bx) = (a+b) + by$$

H/W · 9 15/03/11

$\mathbb{F}$ field $p(x) = a_n x^n + \dots + a_1 x + a_0$ $a_n \neq 0$

polynomial of deg. n / $\mathbb{F}$ ($a_i \in \mathbb{F}$

Question: when is $\mathbb{F}[x]/p(x)$ a field?

Answer: Coming soon $\Leftrightarrow$ $p(x)$ is irred. / $\mathbb{F}$

Prop. $\boxed{\text{Any element of } \mathbb{F}[x]/p(x) \text{ can be represented uniquely by a polynomial of } \deg \leq n-1}$

Proof: Write $I = (p(x)) = \{\lambda(x) p(x) . \lambda(x) \in \mathbb{F}[x]\}$

I Element of $\mathbb{F}[x]/p(x) = \mathbb{F}[x]/I$

are represented in form $a(x) + I$ $a(x) \in \mathbb{F}[x]$

If $\deg a \geq n$ div. $a(x)$ by $p(x)$

necessary our problem $a(x) = \underbrace{q(x)\, p(x)}_{I} + a'(x)$ $\deg a'(x) \leq n-1$

So $a'(x) + I = a(x) + I$ and I've represented $a(x) + I$ in desired form

II This prop. rep. is unique because of

$a'(x) + I = a''(x) + I$

and $\deg(a') \leq n-1$. $\deg(a'') \leq n-1$

$a'(x) - a''(x) \in I$ and $\deg(a' - a'') \leq n-1$

$a'(x) - a''(x) = \lambda(x) p(x)$ $\deg p = n$

So $\lambda(x) = 0$ and $a''(x) = a'(x)$ Q.E.D.

Corollary $\boxed{\mathbb{F}[x]/p(x)\ (\deg p = n) \text{ is a vector space}/\mathbb{F} \text{ and } \dim(\mathbb{F}[x]/p(x)) = n}$

работа
дом. бо!
до следваща

Proof: Every element of $\mathbb{F}[x]/p(x)$ is represented uniquely in form

$$a_0 \cdot 1 + a_1 x + \dots + a_{n-1} x^{n-1} (+ I)$$

so $1, x, \dots, x^{n-1}$ is a basis for $\mathbb{F}[x]/p(x)$

Q.E.D.

Intermediate Stage

Def-n A commutative ring R is said to be an *integral domain*, when

for $a \in R$, $b \in R$: $ab = 0 \Rightarrow (a = 0)$ or $(b = 0)$

Note: every field is a integral domain, but not all integral domain is a field.

$(ab = 0$ and $a \neq 0 \Rightarrow a^{-1}ab = 0 \Rightarrow b = 0)$

e.g.
1) Any field is an integral domain
2) $\mathbb{Z}$ is an int. d.
3) If $\mathbb{F}$ is a field $\Rightarrow \mathbb{F}[x]$ is an integral d.
4) $\mathbb{Z}/4$ is <u>not</u> an integral d.
   $2 \cdot 2 = 0$ but $2 \neq 0$.

Def-n If $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ $a_n \neq 0$
say that $p(x)$ is <u>irred.</u> over $\mathbb{F}$
when there is no factorization $p(x) = a(x) b(x)$ $a(x), b(x) \in \mathbb{F}[x]$

and $\deg(a) < n$ and $\deg(b) < n$

Intermediate prop.

Let $\mathbb{F}$ be a field

$p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{F}[x]$ $\quad a_n \neq 0$

$\therefore$ $\mathbb{F}[x]/p(x)$ is an integral domain iff $p(x)$ is irred. $/\mathbb{F}$

Proof:

$\{\Rightarrow\}$

Suppose $p(x)$ is reducible i.e. $p(x) = a(x)b(x)$, $\deg a < n$, $\deg b < n$

i.

$I = (p(x))$

$(a(x) + I)(b(x) + I) = a(x)b(x) + I = p(x) + I = I = 0$

but $a(x) + I \neq 0$

$b(x) + I \neq 0$

QED.

$\{\Leftarrow\}$

Suppose $p(x)$ is irred. $/\mathbb{F}$

suppose $(a(x) + I)(b(x) + I) = 0$

i.e. $a(x)b(x) + I = 0$

i.e. $a(x)b(x) \in I$

i.e. $a(x)b(x) = \lambda(x) p(x)$ for some $\lambda(x)$ in $\mathbb{F}(x)$

Let $a(x) = a_1(x) \dots a_m(x)$

$b(x) = b_1(x) \dots b_n(x)$

factorization into irred.

$\lambda(x) p(x) = a_1(x) \dots a_n(x)\, b_1(x) \dots b_n(x)$

By uniqueness of factorization
$p(x) = a_i(x)$ or $p(x) = b_j(x)$ for some i, j

If $p(x) = a_i(x)$ $a(x) \in (p(x)) = I$
so $a(x) + I = 0$

if $p(x) = b_j(x)$ $b(x) \in (p(x)) = I$
so $b(x) + I = 0$

$(a(x) + I)(b(x) + I) = 0$
$\Rightarrow a(x) + I = 0$ or $b(x) + I = 0$ Q.E.D

Prop: Let R be a commutative integral dom.

Suppose R contains a field $\mathbb{F}$ (as a subring)
[$\dim_{\mathbb{F}}(R)$ is finite.]

then R is a field

Proof.
1) [illegible] field.
2) lin ?

Let $a \in R$ and $a \neq 0$
Have to show $\exists b \in R$ s.t. $ab = 1$
Let $T : R \to R$
$T(x) = ax$
T is linear over $\mathbb{F}$

So $\dim \operatorname{Ker} T + \dim \operatorname{Im} T = \dim R$

what is $\operatorname{Ker} T$?

$T(a) = 0 \Rightarrow ax = 0$

~~But~~ $a \neq 0$ and R integral domain

so $x = 0$

$\operatorname{Ker} T = \{0\}$

So $\dim \operatorname{Im} T = \dim R$

So $\operatorname{Im} T = R$ (f.d)

T is surjective

So $\exists b \in R \quad T(b) = 1$

i.e. $\exists b \in R \quad ab = 1$

R is a field QED.

Corollary $(\deg p = n)$

$\mathbb{F}[x]/p(x)$ is a field $\Leftrightarrow \mathbb{F}(x)/p(x)$ integral domain

$\Leftrightarrow p(x)$ irred.

13/03/11

Theorem

Let $\mathbb{F}$ be a field

Let $p(x) \in \mathbb{F}[x]$, $\deg(p) = n > 0$

Then following are equivalent:

(i) $\mathbb{F}(x)/p(x)$ is a field

(ii) $\mathbb{F}(x)/p(x)$ is an integral domain

(iii) $p(x)$ is irreducible over $\mathbb{F}$

Proof:

(i) $\Rightarrow$ (ii) is obvious

(ii) $\Rightarrow$ (i) in this case because $\mathbb{F}(x)/p(x)$ is a vector space of finite dimension n over $\mathbb{F}$

I showed last time that (ii) ⇒ (iii) QED

Beware Hypothesis of finite dimensionalites is essential here.

$\mathbb{F}[x]$ has ∞ dim $/\mathbb{F}$
$\mathbb{F}[x]$ is an integral domain but not a field.

Examples: 1) $\mathbb{F} = \mathbb{C}$
let $p(x) \in \mathbb{C}[x]$, when $p(x)$ is irreducible?

best proof: samuel's Alg No theory

Answer: Fundamental theorem of Algebra. Gauss or d'Alembert
iff $p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$
$p(x) = a_n(x-\lambda_1)\dots(x-\lambda_n)$ for some $\lambda_i \in \mathbb{C}$

2) $\mathbb{F} = \mathbb{R}$

let $p(x) \in \mathbb{R}[x]$
when is $p(x)$ irred $/\mathbb{R}$
$p(x) = c(x-\lambda)$ $\lambda \in \mathbb{R}$
$p(x) = ax^2 + bx + c$

Real Question: given $a(x) \in \mathbb{R}[x]$
3) when is $a(x)$ irred. over $\mathbb{Q}$?
No general answers except for an algorithm (boring, but useful)

However there is a trick which ~~gives~~ quite often works.

8.2 **Thm** Eisenstein's criterion

Let $a(x) = a_n x^n + \dots + a_1 x + a_0$
be a polynomial over $\mathbb{Z}$ $(a_i \in \mathbb{Z})$
Suppose there is a prime p s.t.
(i) $a_n \not\equiv 0 \mod p$
(ii) $a_r \equiv 0 \mod p \quad 0 \le r \le n-1$
(iii) $a_0 \not\equiv 0 \mod p^2$

then $a(x)$ is irreducible $/ \mathbb{Q}$

Example 1) (Pythagoras)
Let p be prime then is
$x^2 - p$ is irred $/ \mathbb{Q}$
So $\mathbb{Q}[x]/x^2-p$ is a field.

$\mathbb{Q}[x]/x^2-p \cong a + b\sqrt{p} \quad a, b \in \mathbb{Q}$
$x^2 = p \Leftarrow \sqrt{p} = x \quad (\sqrt{p})^2 = p$

2) $p = 7$
$x^5 + 14x^4 - 21x^2 + 35x + 7$ is irred $/ \mathbb{Q}$

another trick:
$x^4 + 4x^3 + 6x^2 + 4x + 3 = f(x)$ is irred $/ \mathbb{Q}$
$(x+1)^4 + 2 = f(x)$

Write $g(y) = y^4 + 2$
and it is irred $/ \mathbb{Q}$
by Eisenstein

$f(x) = g(x+1)$

$f(x-1) = g(x)$

If $f(x)$ were reducible : $f(x) = a(x)\, b(x)$
$g(x) = a(x-1)\, b(x-1)$ would be also reducible

As g is irreduc. so is f.

Cyclotomic polynomials

$x^n - 1$. We shall show how to factorise completely over $\mathbb{Q}$

First case : $x^p - 1$ $\quad$ p prime

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$$

Define : $C_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ when p is prime

Prop. when p is prime
$C_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ is irred over $\mathbb{Q}$

Proof $\quad C_p(x) = \dfrac{x^p - 1}{x - 1}$

make change of variables $x = y + 1$

$$(y+1)^p = y^p + \sum_{r=1}^{p-1} \binom{p}{r} y^r + 1$$

$$\frac{(y+1)^p - 1}{y} = y^{p-1} + \sum_{r=1}^{p-1} \binom{p}{r+1} y^{r+1} = g(y)$$

Then $g(y)$ satisfies Eisenstein

$\Phi_p(x) = q(x-1)$.
So since q is irred/$\mathbb{Q}$
$\therefore$ Φ_p is irred/$\mathbb{Q}$ **Q.E.D**

Proof of Eisenstein Criterion

stage 1:
If $a(x) = a_n x^n + \dots + a_1 x + a_0$ $\quad a_i \in \mathbb{Z}$
$a_n \not\equiv 0 \mod p$
$a_r \equiv 0 \mod p \quad 0 \le r \le n-1$
$a_0 \not\equiv 0 \mod p^2$

Then $a(x)$ has no proper factorization over $\mathbb{Z}$

Proof of stage I:
Suppose $a(x) = b(x)c(x)$ is a proper factorisation over $\mathbb{Z}$
i.e. $b(x) = b_m x^m + \dots + b_1 x + b_0 \quad b_m \ne 0$
$c(x) = c_k x^k + \dots + c_1 x + c_0 \quad c_k \ne 0$
and $m < n$ so $k < n$ $\quad k + m = n$

First compare constant terms
$a_0 = b_0 c_0$
$a_0 \equiv \mod p \quad a_0 \not\equiv 0 \mod p^2$
so either $p \mid b_0$ & $p \nmid c_0$ or
$p \mid c_0 \dots p \nmid b_0$
wlog. take 1 option.

Next look at coeff of x.
$a_1 = b_1 c_0 + b_0 c_1$
$a_1 \equiv 0 \mod p$ by hypothesis
$b_0 \equiv 0 \mod p$ by choice

so $b_1 c_0 \equiv 0 \mod p$

But $c_0 \not\equiv 0 \mod p$ so $b_1 \equiv 0 \pmod p$

Claim, by induction each $b_r \equiv 0 \mod p$
can assume $b_0 \equiv 0 \mod p$ // induction base
$b_1 \equiv 0 \mod p$

Suppose $b_t \equiv 0 \mod p$ $t \leq r-1$
Look at coeff. of x^r
$$a_r \equiv b_r c_0 + \sum_{t=0}^{r-1} b_t c_{r-t}$$
Inductively $\sum_{t=0}^{r-1} b_t c_{r-t} \equiv 0 \pmod p$

$$a_r \equiv 0 \pmod p$$

But $c_0 \not\equiv 0 \mod p$ so $b_r \equiv 0 \mod p$

so for each r $0 \leq r \leq m$ $(< n)$
$b_r \equiv 0 \mod p$
so $b_m \equiv 0 \mod p$

Compare coeffs of x^n
$a_n = b_m c_n$
so $a_n \equiv 0 \mod p$

Contradiction: so $a(x)$ has no proper factorisation
QED.

Eisenstein Stage II

If $a(x) \in \mathbb{Z}[x]$ has no proper factorization $/\mathbb{Z}$
then $a(x)$ has no proper factorization $/\mathbb{Q}$

Def-n

Let $a(x) = a_n x^n + \dots + a_1 x + a_0$ $\quad a_n \neq 0$
whose $a_i \in \mathbb{Z}$

By $c(a)$ we mean
$c(a) = HCF(a_n, \dots, a_1, a_0)$ } Content of $a(x)$

Easy to see that if $\alpha(x) \in \mathbb{Z}[x]$ can write
$\alpha(x) = c(\alpha)\, a(x)$
where $a(x) \in \mathbb{Z}[x]$, $\boxed{c(a) = 1}$ → trick
Take out communal factors.

e.g. $\alpha(x) = 6x^2 + 96x + 72$
$= 6(x^2 + 16x + 12)$
$= c(\alpha)\,(a(x))$ $\quad | \; c(a) = 1$

Prop. Gauss's Lemma

If $a(x), b(x) \in \mathbb{Z}[x]$, then $c(ab) = c(a)\,c(b)$

corollary

Proof By above trick E.T.P.
$\boxed{\text{if } c(a) = 1 \text{ and } c(b) = 1 \text{ then } c(ab) = 1}$

So write $a(x) = a_n x^n + \dots + a_1 x + a_0$
$b(x) = b_l x^l + \dots + b_1 x + b_0$

$c(a) = 1 = c(b)$

$c(a) = 1 = c(b)$

Must show that if p is a prime, then there is at least one coeff of $a(x)b(x)$ which p does not div.

Since $C(a) = 1$, choose r: $p \nmid a_r$ but $p \mid a_t$ for $t < r$

Since $C(b) = 1$ choose s $p \nmid b_s$ but $p \mid b_t$ $t < s$

coeff of x^{r+s} in $b(x)a(x)$ become

$$= a_r b_s + \sum_{t=r} a_t b_{r+s-t} + \sum_{t<s} a_{r+s-t} b_t$$

by choice $a_r b_s \not\equiv 0 \mod p$,

but $\sum_{t<r} a_t b_{r+s-t} \equiv 0 \mod p$

and also

$\sum a_{r+s-t} b_t \equiv 0 \mod p$

coeff of x^{r+s} in $a(x)b(x)$ is $\not\equiv 0 \mod p$

$c(ab) = 1$ Q.E.D.

27/03/11

Proof of ~~corollary~~ proposition - gauss's lemma

Write $a(x)b(x) = c\,\gamma(x)$, where $c(\gamma) = 1$

So $c = c(a, b)$

Write $a(x) = c_1 \tilde{a}(x)$

$$b(x) = c_2 \tilde{b}(x)$$
$$c(\tilde{a}) = c(\tilde{b}) = 1$$
$$a(x)\,b(x) = c_1 c_2\, \tilde{a}(x)\,\tilde{b}(x)$$
But $c(\tilde{a}\tilde{b}) = 1$

Compare $\left\{ \begin{array}{l} a(x)\,b(x) = c_1 c_2\, \tilde{a}(x)\,\tilde{b}(x) \\ a(x)\,b(x) = c\,\gamma\,x \end{array} \right\}$ so $c = c_1 c_2$

QED

Corollary

$$\boxed{\begin{array}{ll} \underline{\text{if}} & p(x) \in \mathbb{Z}[x] \quad \deg(p) = n \\ \underline{\text{suppose}} & p(x) = \alpha(x)\,\beta(x) \\ & \alpha(x), \beta(x) \in \mathbb{Q}[x],\ \deg \alpha = m \quad \deg \beta = k \\ & \qquad\qquad m + k = n \\ \underline{\text{then}} & p(x) = a(x)\,b(x) \quad \text{where } a(x)\ b(x) \in \mathbb{Z}[x] \\ \& & \deg a(x) = \deg \alpha = m, \quad \deg b = \deg \beta = k \end{array}}$$

Proof:

Assume $c(p) = 1$

clear factors in α, β and write $A(x) = D\,\alpha(x)$
$B(x) = D'\,\beta(x)$,

where D, D' non-zero integer; $A(x), B(x) \in \mathbb{Z}[x]$

$\therefore\ DD'\,p(x) = A(x)\,B(x)$

write $c = c(A)$ $\quad c' = c(B)$

so $A(x) = c\,a(x)$ $\quad c(a) = 1$
$B(x) = c'\,b(x)$ $\quad c(b) = 1$

and $a, b \in \mathbb{Z}[x]$

$$DD'\,p(x) = cc'\,a(x)\,b(x)$$

DD' = Content LHS $\qquad DD' = cc'$
cc' = content RHS

so $p(x) = a(x)\,b(x)$ as claimed

If $c(p)=1$, then write $p(x)=c(p)\,\tilde{p}(x)$

$c(\tilde{p})=1$

$\tilde{p}(x)=\frac{1}{c(p)}\,p(x)$

(& proceed as above) **QED**

Corollary $\boxed{\text{\underline{If} } p(x)\in\mathbb{Z}[x] \text{ \underline{then} } p(x) \text{ has no proper factorization over } \mathbb{R} \text{ iff } p(x) \text{ has no proper factorisation } /\mathbb{Q}}$

Corollary $\boxed{\text{\underline{If} } p(x)\in\mathbb{Z}[x] \text{ satisfies Eisenstein \underline{then} it is irred } /\mathbb{Q}}$

Application: How to factorise x^n-1 completely $/\mathbb{Q}$

Over $\mathbb{C}$: Take $\zeta_n=\exp\left(\frac{2\pi i}{n}\right)=\zeta$

So $x^n-1=(x-1)(x-\zeta)(x-\zeta^2)\dots(x-\zeta^{n-1})$

$S^1=\{z\in\mathbb{C} \ |z|=1\}$

Obviously $\mathrm{ord}(\zeta_n^k)$ divides n

Let d be a divisor of n

Define $\Phi_d(x)=\prod\limits_{\mathrm{ord}(\zeta_n^r)=d}(x-\zeta_n^r)$

It turns ~~of~~ out that each $c_d(x) \in \mathbb{Z}[x]$
and $c_d(x)$ ~~is~~ irred./$\mathbb{Q}$,

So now: $x^n - 1 = \prod_{d \mid n} c_d(x)$

<u>So let's go!!</u> $x-1 = c_1(x)$

So far $\Rightarrow$

$c_1(x) = x-1$
$c_2(x) = x+1$
$c_3(x) = x^2+x+1$
$c_4(x) = x^2+1$
$c_5(x) = x^4+x^3+x^2+x-1$
$c_6(x) = x^2-x+1$
$c_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$
$c_8(x) =$
$c_9(x) =$
$c_{10}(x)$
$c_{11}(x)$
$c_{12}(x)$

$x^2-1 = (x-1)(x+1)$
$x^2-1 = c_1(x)\,c_2(x)$
So $c_2(x) = x+1$
$x^3-1 = c_1(x)\,c_3(x)$
$\quad = (x-1)(x^2+x+1)$
$x^4-1 = c_1(x)\,c_2(x)\,c_4(x)$
$\quad = (x-1)(x+1)\,c_4(x)$
$\quad = (x^2-1)(x^2+1)$

$c_5 = \frac{x^5-1}{x-1}$ $\quad x^5-1 = c_1(x)\,c_5(x)$
$\quad = (x-1)(x^4+x^3+x^2+x+1)$
$x^6-1 = c_1(x)\,c_2(x)\,c_3(x)\,c_6(x)$
$\quad = (x^3-1)(x+1)\,c_6(x)$ $\quad$ or $\frac{x^6-1}{(x^3-1)} = (x+1)c_6$
$\quad = (x^4+x^3-x-1)\,c_6(x)$
$\quad = (x^4+x^3-x-1)(x^2-x+1)$
$\quad = (x^3-1)(x+1)(x^2-x+1)$
$x^7-1 = c_1(x)\,c_7(x)$
$\quad = (x-1)\,c_7(x)$
$x^8-1 = c_1 c_2 c_4 c_8$
$\quad = (x^4-1)\,c_8$
$x^9-1 = c_1 c_3 c_9$
$\quad = (x^3-1)\,c_9$

give complete factorization $x^{?}-1$ / $\mathbb{Q}$

$$x^{15}-1 = C_1 C_2 C_3 C_6 C_9 C_{18}$$
$$= (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^3+1)C_{18}$$
$$= (x^6-1)(x^6+x^3+1)\,C_{18}$$
$$= (x^6-1)(x^6+x^3+1)(x^6-x^3+1)$$

$$\frac{x^{15}-1}{x^6-1} = x^{12}+x^6+1$$

$$\frac{y^3-1}{y-1} = y^2+y+1$$

So $C_{18}(x) = \left(\dfrac{x^{12}+x^6+1}{x^6+x^3+1}\right) = x^6-x^3+1$

$$\begin{array}{r}
x^6-x^3+1 \\
x^6+x^3+1 \;\big)\; x^{12} \qquad x^6 \qquad 1 \\
\underline{x^{12}+x^9+x^6} \\
-x^9 \quad +1 \\
\underline{-x^9 - x^6 - x^3} \\
x^6+x^3+1
\end{array}$$

x^n+1 ?

$(x^{2n}-1) \; (x^n-1)(x^n+1)$

$\left(\dfrac{x^{2n}-1}{x^n-1}\right) = x^n+1$ & new factors $\dfrac{x^{2n}-1}{x^n-1}$

& cancel

Algebra: Revision on lecture 25/03/11

(0) $Aut(C_p) \cong C_{p-1}$

(I) If $\mathbb{F}$ is a field and $G \subset \mathbb{F}^* = \{x \in \mathbb{F} : x \neq 0\}$ G finite subgroup $\Rightarrow$ G is cyclic

(II) If $\mathbb{F}$ is a field, $G \subset \mathbb{F}^*$ is subgroup and $|G| = p^n \Rightarrow G$ is cyclic

Theorem: Let p be a prime, $\mathbb{F}$ is field, $G \subset \mathbb{F}^*$ is a subgroup. If $|G| = p^n$ then G is cyclic

Proof: If $x \in G$ ord$(x) = p^e$ for some $e \leq n$

Let $m = \max\{e : \exists x \in G \ \text{ord}(x) = p^e\}$

Then $m \leq n$

Choose $y \in G$: ord $y = p^m$

Then <u>every</u> element $x \in G$ satisfies

$x^{p^m} = 1$

Look at equation $x^{p^m} - 1$ over $\mathbb{F}$

It has at most p^m solutions

But <u>every</u> element $x \in G$ satisfies eq-n

So $|G| \leq p^m$. But $|G| = p^n$

So $p^n \leq p^m$ so $n \leq m$ & $m \leq n$ So $m = n$

But y has ord$(y) = p^m = p^n$

i.e. $|G| = p^n$ and contains y with ord$(y) = p^n$

so $G \cong C_{p^n}$ with y as generator. QED

Corollary: If $\mathbb{F}$ is a field and $G \subset \mathbb{F}^*$ is a finite subgroup, then G is cyclic

Proof: Write $|G| = p_1^{e_1} \cdots p_m^{e_m}$ where $p_1 \ldots p_m$ are distinct primes

By Sylow, G has a subgroup G_i with $|G_i| = p_i^{e_i}$

But G is abelian so $(G_i \triangleleft G)$

~~So g~~

So $G_i G_j = G_j G_i$ for all i, j

So $G_i G_j$ is a subgroup of G

Claim by induction on m that $G \cong G_1 \times \dots \times G_m$

For $m = 1$ nothing to prove

Suppose true for $m-1$, put $G' = G_1 G_2 \cdots G_{m-1}$

G' is a subgroup of G and G

$G' \cong G_1 \times \dots \times G_{m-1}$ by induction

Consider $\psi : G' \times G_m \to G$

$(x, y) \to xy$

ψ is injective because

$\operatorname{ord}(x) = p_1^{f_1} \cdots p_{m-1}^{f_{m-1}}$ for some f_i

$\operatorname{ord}(y) = p_m^{f_m}$ $\operatorname{ord}(y^{-1}) = p_m^{f_m}$

If $xy = 1$

$p_m^{f_m} = \operatorname{ord}(y^{-1}) = \operatorname{ord}(x) = p_1^{f_1} \cdots p_{m-1}^{f_{m-1}}$

and $p_1 \dots p_m$ distinct primes

Contradiction, so $xy = 1 \Rightarrow x = 1, y = 1$

$\Rightarrow (x, y) = (1, 1) = n$

But $|G' \times G_m| = |G'|\,|G_m| = |G|$ so ψ is surjective

So $G \cong G_1 \times \dots \times G_m$) by previous result

$= G_{p_1^{e_1}} \times \dots \times G_{p_m^{e_m}}$

$\cong G_N$ $\quad N = p_1^{e_1} \cdots p_m^{e_m} = |G|$ Q.E.D.

Corollary Let p be a prime

$\mathbb{F}_p$ field with p elements

$\Rightarrow \mathbb{F}_p^* \cong C_{p-1}$

Proof $|\mathbb{F}_p^*| = p - 1$ & use last result Q.E.D.

Proof: Now take ~~G~~ $C_p = \{1, a, \dots, a^{p-1}\}$ $a^p = 1$

Let $\varphi_r : C_p \to C_p$, $\varphi_r(a) = a^r$

$\operatorname{Aut}(C_p) = \{\varphi_1, \varphi_2, \dots, \varphi_{p-1}\}$

25/03/11

$= \mathbb{F}_p^* = \{1, \dots, p-1\}$
$\cong C_{p-1}$ QED.

We've shown:
thm If p is prime $\Rightarrow Aut(C_p) \cong C_{p-1}$ $\square$

additive group — all homomorphism ~~mult monoid~~

$\mathbb{F}_p \longrightarrow Hom(C_p, C_p)$
$r \longrightarrow (a \to a^r)$

'exp'$(r) = a^r$ $0 \to id$