# Math 322, lecture 16, 2/11/17

Last time: $G$ order 6.

$P < G$ order 2 } ← Cauchy's thm
$Q < G$ order 3.
counting argument
Then $Q$ is normal, $G = PQ$ so $G = P \ltimes Q$.
work
$P \cap Q = \{e\}$ ← Lagrange's thm

if $x, x' \in P$, $y, y' \in Q$ then

$$(x'y')(xy) = x'x\left((x^{-1}y'x)\, y\right)$$

so mult in $G$ determined by map $(x, y) \mapsto xyx^{-1}$
= action of $P$ on $Q$ by automorphisms

Say $P = \{1, x\}$, $Q = \{1, y, y^2\}$

$1 \in P$ acts trivially on $Q$.
$x$ acts on $Q$ as follows: $x \cdot 1 x^{-1} = 1$

and either $\begin{cases} xyx^{-1} = y^2 \\ xy^2x^{-1} = y \end{cases}$

or $\begin{cases} xyx^{-1} = y \\ xy^2x^{-1} = y^2 \end{cases}$

In the second case, $xy = yx$
$xy^2 = y^2x$

so mult rule is $(x^{a'}y^{b'})(x^a y^b) = x^{a+a'} y^{b+b'}$ $(xy = yx)$
so $G \cong C_2 \times C_3 \cong C_6$ (CRT)

In the first case, $xyx^{-1} = y^{-1}$ $\quad (y^2 = y^{-1})$

$xy^2x^{-1} = (y^2)^{-1}$ $\quad y = (y^2)^{-1}$

so $G = C_2 \ltimes C_3 = \langle x, y \mid x^2 = 1, y^3 = 1, xyx^{-1} = y^{-1} \rangle$

$\cong D_6$

G ~~has~~ generated by x of order 2, y of order 3 and $xyx^{-1} = y^{-1}$!

General case: G of order $pq$

---

Here $p < q$ are primes

By Cauchy's thm, G has subgps P, Q of order $p, q$ respectively. By Lagrange's thm, $\#(P \cap Q) = 1$ (it must divide both $p, q$), so map $P \times Q \to PQ \subset G$ is a bijection,

so $PQ = G$, with unique representation

Let $Q'$ be another subgroup of order $q$. If $Q \neq Q'$ then $Q \cap Q'$ is a proper subgp of both, i.e. $\{e\}$, then $\#(QQ') = q^2 > pq = \#G$ is a contradiction, so $Q' = Q$.

Now for any $g \in G$, $gQg^{-1}$ is a subgp of order $q$,

so $gQg^{-1} = Q$, and $Q$ is normal

<u>Summary</u>: $G \cong P \ltimes Q$, need to classify actions of $P$ on $Q$ by gp autos

Fix generators $x, y$ of $P, Q$ respectively.
For $a \in \mathbb{Z}/p\mathbb{Z}$, $b \in \mathbb{Z}/q\mathbb{Z}$ general element of $G = PQ$ has the form

$$x^a y^b$$

then

$$(x^{a'} y^{b'}) \cdot (x^a y^b) = x^{a'+a} (x^{-a} y^{b'} x^a) y^b$$

still need to compute $x^{-a} y^{b'} x^a$.

But: $x^{-a} y^{b'} x^a = (x^{-a} y x^a)^{b'}$

And $x^{-a} y x^a = \underbrace{x^{-1}(x^{-1}(\ldots x^{-1}}_{a}(y)\underbrace{x)x \ldots)x}_{a}$

So enough to know $xyx^{-1}$! Now $xyx^{-1} \in Q$ so there is $k \pmod q$ s.t. $xyx^{-1} = y^k$.

Then

$$x^2(y)x^{-2} = x(xyx^{-1})x^{-1} = xy^kx^{-1} = (xyx^{-1})^k = (y^k)^k = y^{k^2}$$

$$x^3(y)x^{-3} = x(x^2yx^{-2})x^{-1} = x(y^{k^2})x^{-1} = (xyx^{-1})^{k^2} = (y^k)^{k^2} = y^{k^3}$$

by induction

$$x^a y x^{-a} = y^{k^a}, \quad x^{-a} y x^a = y^{k^{-a}}$$

to make sense of this note that $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ since $y^k$ must also be a generator of $Q$ (conjugation by $x$ is an automorphism).

If $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ then $k^{-a}$ makes sense for $a \in \mathbb{Z}$

Conclusion: given $k$, mult. in $G$ is:

$$(x^{a'}y^{b'})\cdot(x^{a}y^{b}) = x^{a'+a}\, y^{b'k^{-a}+b}$$

Constraint on $k$: $x^p = 1$ so $y = x^p y x^{-p} = y^{k^p}$

so must have $k^p = 1$ in $(\mathbb{Z}/q\mathbb{Z})^\times$

Case 1: $k = [1]_q$, i.e. $xyx^{-1} = y$ or $xy = yx$

then the mult. rule is:

$$(x^{a'}y^{b'})\cdot(x^{a}y^{b}) = x^{a'+a}\, y^{b'+b}$$

i.e. $G \cong C_p \times C_q \cong C_{pq}$

Case 2: $k \neq [1]_q$ (Example: $k = [-1]_q$, $p=2$ so $k^2 = [1]$, then $xyx^{-1} = y^{-1}$, so $G \cong D_{2q}$ (only $\pm 1$ satisfy $k^2 \equiv 1\ (q)$))

If $k \neq [1]_q$ but $k^p = [1]$, order of $k$ in $(\mathbb{Z}/q\mathbb{Z})^\times$ is $p$

Lagrange's thm: order of $k \mid$ order of $(\mathbb{Z}/q\mathbb{Z})^\times$

i.e. $p \mid q-1$

i.e. $q \equiv 1\ (p)$

So if $q \not\equiv 1\ (p)$ then $k = [1]$, $G$ is cyclic of order $pq$.

Examples: If $\#G = 15$ then $G \cong C_{15}$: $15 = 3\cdot 5$ and $5 \not\equiv 1\ (3)$

If $q \equiv 1\ (p)$ then $p \mid q-1$ so by Cauchy's thm
there <u>is</u> $k \in (\mathbb{Z}/q\mathbb{Z})^\times$ of order $p$.
(in fact there are $p-1$ of them)

---

<u>Fact:</u> $q$ prime (or power of an odd prime)
then $(\mathbb{Z}/q\mathbb{Z})^*$ is cyclic.

Pf: Say $q$ is prime, so $\mathbb{Z}/q\mathbb{Z}$ is field, so for any $d \mid q-1$, equation $x^d = 1$ has at most $d$ roots
if $x \in (\mathbb{Z}/q\mathbb{Z})^\times$ has order $d$ then $\langle x \rangle$ must be those roots
so $(\mathbb{Z}/q\mathbb{Z})^\times$ has at most 1 subgp of order $d$ for any $d \mid q-1$
so $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic.

---

So if $p \mid q-1$, $(\mathbb{Z}/q\mathbb{Z})^\times$ has a <u>unique</u> subgp of order $p$

Say conjugation by $x$: $y \to y^k$
then " " $x^a$ : $y \mapsto y^{k^a}$

and $\{k^a\}_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} = \left\{ \begin{array}{l} \text{non-identity} \\ \text{elements of } \langle k \rangle \end{array} \right\}$

But both $x, x^a$ are generators of $P \simeq C_p$
so up to choice of generator of $P$, all values of $k$ occur (if one does)

Summary: If $\# G = pq$ then

(1) If $q \not\equiv 1 (p)$, $G \simeq C_{pq}$

(2) If $q \equiv 1 (p)$ either $G \simeq C_{pq}$ or $G \simeq \langle x, y \mid x^p = 1, y^q = 1, xyx^{-1} = y^k \rangle$

where $k^p \equiv 1 (q)$, if such a group exists.

Proof of existence:

Pf 1: check by hand mult rule from before

Pf 2: The map $x^a \mapsto (y \mapsto y^{k^a})$
is a hom $\varphi: C_p \to \mathrm{Aut}(C_q) \Leftrightarrow$ action of $C_p$ on $C_q$ by gp automorphisms

check: If $H, N$ gps, $\varphi: H \to \mathrm{Aut}(N)$ a hom

then defining $(h', n') \cdot (h, n) = (hh', (\varphi(h^{-1}))(n') \cdot n)$

gives a group structure on the set $H \times N$

where $\{(h,1)\}_{h \in H}$ is a subgp isom to $H$

$\{(1,n)\}_{n \in N}$ " " " " " $N$

$(h,1)(1,n)(h^{-1},1) = (1, (\varphi(h))(n))$

(Ken problem of PS8)