13/10

classify all groups of order

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

$\downarrow$ pq

Proposition

Let p, q be primes with $p > q$, and $q \nmid p-1$ and let G be a group of order pq

Then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$

(proof)

By Cauchy's theorem, there exists $a \in G$ and $b \in G$ such that $o(a) = p$ and $o(b) = q$

$H = \langle a \rangle$, $K = \langle b \rangle$

Then $|H| = p$, $|K| = q$ $\Rightarrow |H \cap K| = 1$

$\Rightarrow |HK| = pq$ $\Rightarrow$ $HK = G$

Any element of G can be written as $g = hk$ for some $h \in H$, $k \in K$ $= a^i b^j$

$\Rightarrow G = \langle a, b \rangle$

Number of Sylow-p subgroups $= n_p$

$n_p \mid pq$ and $n_p \equiv 1 \mod p$

$\Rightarrow n_p \mid q$

$\Rightarrow n_p = 1$ (or) $n_p = q$

$n_p = q$ is a contradiction $(p > q)$

$\Rightarrow n_p = 1$

$\Rightarrow H \trianglelefteq G$ [H is the only Sylow p subgroup]

(i) $H \trianglelefteq G$, $K \leq G \Rightarrow HK \leq G$

(ii) $G = HK$ and $H \cap K = (1)$

Since $H \trianglelefteq G$, $bab^{-1} = a^s$ for some $0 \leq s < p$

$a = b^q a b^{-q}$

Apply induction, we have $a = a^{s^q}$

$\Rightarrow p \mid s^q - 1$

For the equation $x^q - 1 = 0$ in $\mathbb{Z}/p\mathbb{Z}$
's' is a solution

$o(s)$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is ?

$o(s) \mid p-1$ and $o(s) \mid q \Rightarrow o(s) = 1$

$\Rightarrow bab^{-1} = a$

$\Rightarrow ba = ab$

Then G is an Abelian group

$H \trianglelefteq G$, and let $b^l \in K$

$gb^lg^{-1} = a^ib^jb^lb^{-j}a^{-1} = b^l$

$\Rightarrow K \trianglelefteq G$

Using $H \trianglelefteq G$, $K \trianglelefteq G$, $G = HK$ and $H \cap K = (1)$

$\boxed{G \cong H \times K}$

Fundamental Theorem of Finite Abelian Groups

If G is a finite Abelian group of order n, then $G = H_1 \oplus H_2 \oplus \cdots H_l$ where $H_1, H_2, \ldots, H_l$ are cyclic groups of order $p_1^n, \ldots, p_l^n$ respectively where $p_1, \ldots, p_l$ are prime numbers

$4 \to \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$6 \to \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

$8 \to \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$12 \to \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$

Let G be an additive group
Let $H, K \leq G$

(i) $H \trianglelefteq G$, $K \trianglelefteq G$
(ii) $H \cap K = (0)$
(iii) $G = H + K$

Then $G \cong H \times K$

We say that G is the direct sum of H and K and write $G = H \oplus K$

Definition

A group G is said to be decomposable if $G = H \oplus K$, for some proper subgroups H and K and indecomposable otherwise.

Proposition

A cyclic group of order p^m is indecomposable

Let G be a group of order p^m

Suppose H, K are proper subgroups such that $G = H \oplus K$

Take $g \in G$, then $g = h + k$ $(h \in H, k \in K)$

WLOG, assume $|H| = p^r$, $|K| = p^s$ $(r, s < m)$ and $r \leq s$

$$p^s(g) = p^s(h+k)$$
$$p^s(g) = 0$$

$\Rightarrow$ p^s is divisible by order of G $(\Rightarrow\Leftarrow)$ $p^m \nmid p^s$

$\Rightarrow$ It is indecomposable

Proposition

If G is an abelian group of order mn, where $(m,n) = 1$ then G is decomposable

(Proof)

Let
$$G(m) = \{g \in G \mid mg = 0\}$$
$$G(n) = \{g \in G \mid ng = 0\}$$

Then
1. $G(m), G(n) \trianglelefteq G$
2. $G = G(m) \oplus G(n)$
3. $G(m) \cap G(n) = 0$

$\gcd(m, n) = 1$

$\Rightarrow mx + ny = 1$ $\Rightarrow$ $xmg + yng = g$

Consider elements xmg, yng

$$n(xmg) = x(mn\,g) = 0 \Rightarrow xmg \in G(n)$$
$$m(yng) = y(mn\,g) = 0 \Rightarrow yng \in G(m)$$

$\Rightarrow G = G(m) \oplus G(n)$

Let $x \in G(m) \cap G(n)$

$\Rightarrow mx = 0$ and $nx = 0$

$\Rightarrow o(x) \mid \gcd(m, n) = 1 \quad \Rightarrow x = 0$

Corollary

If G is an abelian group of order $p^n m$, where $n \geq 1$ and $\gcd(p, m) = 1$, then

$G = G(p^n) \oplus G(m)$

• Previously $G(m) \lneq G$ and $G(n) \lneq G$ (Claim!)

Let p be a prime dividing n

By Cauchy's theorem, there exists $g \in G$ such that $o(g) = p$

If $g \in G(m)$, then $mg = 0$

$\Rightarrow p \mid m$

$\Rightarrow p \mid \gcd(m, n) = 1 \; (\Rightarrow\Leftarrow)$

$\Rightarrow g \notin G(m)$

Proposition

An indecomposable finite Abelian group is a p-group for some prime p.

If $|G| = p^n m$ where $n \geq 1$ and $\gcd(m, p) = 1$

then $G = G(p^n) \oplus G(m) \quad \Rightarrow G(p^n) =$

$G(m) =$

$|G| = N = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$

$G = G(p_1^{r_1}) \oplus \cdots \oplus G(p_s^{r_s})$

$|G(p_1^{r_1})| = p_1^{r_1}$

By Sylow's theorem, G has a subgroup of order $p_1^{r_1}$. For every $h \in H_1$ (H_1 is the subgroup of order $p_1^{r_1}$)

$p_1^{r_1} h = 0 \quad \Rightarrow \quad H_1 \leq G(p_1^{r_1})$

Single element in Sylow p-subgroup of $G(p_1^{r_1})$

$\Rightarrow G(p_1^{r_1}) = H_1$

Q) what are indecomposable Abelian p ~~groups~~ groups?

$$8 \to \begin{cases} \mathbb{Z}/8\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{cases}$$

Proposition

A non trivial finite abelian p-group having a unique cyclic subgroup of order p is cyclic.

(Proof)

Let $m = \max \{ i \mid \exists g \in G,\ o(g) = p^i \}$

Let $o(g) = p^m$

$\Rightarrow o(p^{m-1} g) = 1$ (or) p

$\Rightarrow o(p^{m-1} g) = 1$ ($\Rightarrow\Leftarrow$) $o(g) = p^m$

$\Rightarrow o(p^{m-1} g) = p$

Claim : $G = \langle g \rangle$

If not, then $\langle g \rangle \subsetneq G$ and $p \mid |G/\langle g \rangle|$

there exists an element $b + \langle g \rangle \in G + \langle g \rangle$

such that

$p(b + \langle g \rangle) = \langle g \rangle$

$\Rightarrow pb = \langle g \rangle$

So, $pb = jg$ for some integer j

$p^m b = 0$

$p(p^{m-1} b) = p^{m-1}(jg) = p^{m-1} j (g)$

$p^{m-1}(pb)$

$\Rightarrow p^m \mid p^{m-1} j \Rightarrow p \mid j \Rightarrow j = pk$

$\Rightarrow p(b - kg) = 0$

But $\langle g \rangle$ is the unique cyclic subgroup of order p

$\Rightarrow b - kg \in \langle g \rangle$

$\Rightarrow b \in \langle g \rangle$