Teorema (Cinese del Resto):

$m, n \in \mathbb{Z}$ t.c. $MCD(m,n) = 1 \Rightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{mn\mathbb{Z}}$

Dim.

Definiamo $f : \mathbb{Z} \longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$ t.c.

$$f(k) = ([k]_m, [k]_n) = (k + m\mathbb{Z}, k + n\mathbb{Z})$$

Si ha che:

$$\mathrm{Ker}\, f = \{k \in \mathbb{Z} \mid k[1]_m = [0]_m,\ k[1]_n = [0]_n\}$$
$$\overset{!}{=} \{k \in \mathbb{Z} \mid m \mid k \wedge n \mid k\} = mn\mathbb{Z}$$

$\Rightarrow$ per il teorema di omomorfismo si ha:

$$\exists\, \tilde{f} : \mathbb{Z}/_{\mathrm{Ker}\, f} = \mathbb{Z}/_{mn\mathbb{Z}} \longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \text{ iniettiva}$$

Dato che $|\mathbb{Z}/_{mn\mathbb{Z}}| = mn = |\mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}|$, $\tilde{f}$ è suriettiva $\Rightarrow \tilde{f}$ isomorfismo $\Rightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{mn\mathbb{Z}}$

q.e.d.

esempio (Lemma di Burnside):

1) $|G| = pq$ con p, q primi, $p \nmid (q-1)$, $p < q$. Allora G è ciclico.

$\Rightarrow P$ p-Sylow, Q q-Sylow, allora $|P| = p$, $|Q| = q$, $P \cap Q = \{1\}$

$\Rightarrow s_q = 1 + z \cdot q$ con $z \in \mathbb{Z} \wedge s_q \mid p$

$\Rightarrow s_q = 1 \vee s_q = p$ ma se $p = 1 + zq$ allora $p = 1 + zq < q$ ↯ $\Rightarrow s_q = 1 \Rightarrow Q \trianglelefteq G$

$\Rightarrow s_p \equiv 1 \mod p \wedge s_p \mid q \Rightarrow s_p = 1 \vee s_p = q \wedge s_p = 1 + z'p$

ma se $s_p = q$ allora $q - 1 = z'p$ ↯ $\Rightarrow s_p = 1$

$\Rightarrow P \trianglelefteq G \Rightarrow G \cong P \times Q$ che è ciclico per il Teorema Cinese del resto.

Prodotto "interno" di gruppi:

Siano G gruppo, $A, B \subseteq G$ t.c. $A \trianglelefteq G$, $B \trianglelefteq G$, $A \cap B = \{1\}$ $AB = G$. Allora $G \cong A \times B$ grazie all'isomorfismo così definito:

$$f: A \times B \longrightarrow G$$
$$(a, b) \longmapsto ab$$

verifichiamo che f è isomorfismo:

1) f è omomorfismo:

$$f((a,b)(c,d)) = f(a,b) f(c,d)$$

$\iff acbd = abcd$ ✓

Infatti, se $x \in A$, $y \in B$ allora $xy = yx$:

$$xy(yx)^{-1} = \underbrace{xyx^{-1}}_{\in B} y^{-1} \in B$$
$$= \underbrace{x\, yx^{-1} y^{-1}}_{\in A} \in A$$

$\Rightarrow (xy)(yx^{-1}) \in A \cap B = \{1\} \Rightarrow xy = yx$ ✓

2) f è suriettiva $(G = AB)$ ✓

3) f è iniettiva:

$$\ker f = \{(a,b) \mid ab = 1\}$$
$$= \{(a,b) \mid \underset{A}{\underset{\cap}{a}} = \underset{B}{\underset{\cap}{b^{-1}}}\} \Rightarrow a = b = 1 \Rightarrow \ker f = \{1\}$$ ✓

$\Rightarrow f$ isomorfismo $\Rightarrow G \cong A \times B$

Ciò implica, per esempio, che i gruppi di ordine 15 sono ciclici.

esempio

G t.c. $|G| = 200$. Allora $\exists$ sottogruppo normale proprio non banale di G

$\Rightarrow 200 = 2^3 \cdot 5^2 \Rightarrow s_2 \mid 5^2 \wedge s_2 \equiv 1 \mod 2$ e

$s_5 \mid 2^3 \wedge s_5 \equiv 1 \mod 5 \Rightarrow s_5 = 1, 6, 11, \dots$ ma

$s_5 \mid 8 \Rightarrow s_5 = 1 \Rightarrow$ Un 5-Sylow è normale

Def. (Gruppo Semplice):

Un gruppo G si dice SEMPLICE se non ha sottogruppi normali propri non banali.

esempi

1) $\mathbb{Z}/p\mathbb{Z}$, con p primo, è semplice
2) A_5 è semplice (in generale, A_n con $n \geq 5$ è semplice)
3) Nessun gruppo di ordine dispari (non primo) non banale è semplice, anzi è risolubile.

S_{p^k} ha p-sottogruppi di Sylow.

Ogni gruppo finito è isomorfo ad un sottogruppo di S_{p^k} per un certo k:

se $|G| = n$ allora G è isomorfo ad un sottogruppo di S_n (Cayley). S_n è isomorfo ad un sottogruppo di S_m $\forall m \geq n$.

Teorema:

Se G è sottogruppo di G' t.c. G' ha p-Sylow, allora G ha p-Sylow

Dim.:

Siano $A, B \subseteq G$. Definiamo su $x, y \in G$ la relazione:

$$x \sim y \iff \exists\, a \in A,\ b \in B \text{ t.c. } y = axb$$

$\sim$ è relazione di equivalenza e si ha:

$$[x]_\sim = AxB$$

Quanti elementi ha $[x]_\sim$?

$$|AxB| = |AxBx^{-1}| = |AB| \quad \text{perché } |xBx^{-1}| = |B|$$

mostriamo che $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$:

quando $a_1 b_1 = a_2 b_2$? Supponiamo $c = a_1 b_1 = a_2 b_2$, allora $a_2^{-1} a_1 = b_2 b_1^{-1} \in A \cap B$ ecc...

$$\Rightarrow |AB| \cdot |A \cap B| = |A| \cdot |B| \Rightarrow |AxB| = \frac{|A| \cdot |xBx^{-1}|}{|A \cap xBx^{-1}|} = \frac{|A| \cdot |B|}{|A \cap xBx^{-1}|}$$

$\Rightarrow$ Siano quindi $G \subseteq G'$ sottogruppo e Q un p-Sylow in G'. Allora G ha un p-Sylow della forma

$$P = G \cap xQx^{-1} \text{ per un certo } x \in G'$$

$\Rightarrow |G'| = p^m t'$ con $p \nmid t'$, $|G| = p^n t$ con $p \nmid t$

allora necessariamente $n \leq m$

$\Rightarrow$ Scriviamo ora G' come unione di classi di equivalenza disgiunte (nella relazione vista sopra prendiamo $A = G$, $B = Q$):

$$G' = Gx_1Q \cup Gx_2Q \cup \ldots \cup Gx_rQ$$

$$\Rightarrow |GxQ| = \frac{|G| \cdot |Q|}{|G \cap xQx^{-1}|} = \frac{p^n t\, p^m}{|G \cap xQx^{-1}|}$$

$\Rightarrow |xQx^{-1}| = p^m$ quindi $|G \cap x_iQx_i^{-1}| = p^{m_i}$ con $m_i \leq m$

$\Rightarrow$ mostriamo che, per almeno un i, si ha $m_i = n$:

se fosse $m_i < n$ $\forall i$, allora ogni $|G x_i Q|$ è multiplo di p^{m+1}, quindi $|G'|$ sarebbe multiplo di p^{m+1} $\lightning$ ($|G'| \nmid p^{m+1}$)

$\Rightarrow \exists x \in G'$ t.c. $|G \cap x Q x^{-1}| = p^m$

$\Rightarrow x Q x^{-1}$ è p-Sylow di G.

q.e.d.

esempi:

1) Trovare i 3-Sylow in S_4:

$\Rightarrow$ basta trovare i 3-Sylow in S_9. Dato Q uno di essi, si calcola $S_4 \cap (x Q x^{-1})$ e si trovano tutti i 3-Sylow di S_4.

2) Qual è la massima potenza di p primo che divide $n!$?

$\Rightarrow$ ogni p interi fra 1 ed n contribuiscono un fattore p.

p^2 " " " " " " " " " "

p^3

$\vdots$

ecc.

$\Rightarrow$ la massima potenza di p che divide $n!$ è quindi:

$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots + \lfloor \frac{n}{p^k} \rfloor + \dots$ (dove $\lfloor x \rfloor$ è la parte intera di x)

3) Con quanti 0 finisce $32!$?

Basta contare quale massima potenza di 5 divide $32!$

$\Rightarrow \lfloor \frac{32}{5} \rfloor + \lfloor \frac{32}{5^2} \rfloor = 6 + 1 = 7$

$\left(\lfloor \frac{32}{2} \rfloor + \lfloor \frac{32}{2^2} \rfloor + \lfloor \frac{32}{8} \rfloor + \lfloor \frac{32}{16} \rfloor + \lfloor \frac{32}{32} \rfloor = 31 \right)$

4) Sia $|G| = 6$ non abeliano. Allora:

$$s_2 | 3 \wedge s_2 \equiv 1 \bmod 2 \quad \Rightarrow s_2 = 1 \vee s_2 = 3$$

$$s_3 | 2 \wedge s_3 \equiv 1 \bmod 3 \quad \Rightarrow s_3 = 1$$

$\Rightarrow$ c'è 1 sottogruppo normale di ordine 3.