Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione dell'01-04-2020
(Sezioni 14 e 15 delle dispense)

Osservazione 15.3

Gruppi abeliani di ordine p^k:

$k = 1$ C_p $\mathrm{ab}(p) = 1$

$k = 2$ $C_{p^2},\ C_p^2$ $\mathrm{ab}(p^2) = 2$

$k = 3$ $C_{p^3},\ C_{p^2} \oplus C_p,\ C_p^3$ $\mathrm{ab}(p^3) = 3$

$k = 4$ $C_{p^4},\ C_{p^3} \oplus C_p,\ C_{p^2} \oplus C_{p^2},\ C_{p^2} \oplus C_p^2,\ C_p^4$ $\mathrm{ab}(p^4) = 5$

Osservazione 15.3

Gruppi abeliani di ordine p^k:

$k = 1$ C_p $\quad \mathrm{ab}(p) = 1$

$k = 2$ $C_{p^2},\ C_p^2$ $\quad \mathrm{ab}(p^2) = 2$

$k = 3$ $C_{p^3},\ C_{p^2} \oplus C_p,\ C_p^3$ $\quad \mathrm{ab}(p^3) = 3$

$k = 4$ $C_{p^4},\ C_{p^3} \oplus C_p,\ C_{p^2} \oplus C_{p^2},\ C_{p^2} \oplus C_p^2,\ C_p^4$ $\quad \mathrm{ab}(p^4) = 5$

Gruppi abeliani di ordine 72 ($\mathrm{ab}(72) = \mathrm{ab}(2^3)\mathrm{ab}(3^2) = 3 \cdot 2 = 6$):

- $C_8 \oplus C_9 \cong C_{72}$
- $C_8 \oplus C_3^2 \cong C_{24} \oplus C_3$
- $C_4 \oplus C_2 \oplus C_9 \cong C_{36} \oplus C_2$
- $C_4 \oplus C_2 \oplus C_3^2 \cong C_{12} \oplus C_6$
- $C_2^3 \oplus C_9 \cong C_{18} \oplus C_2^2$
- $C_2^3 \oplus C_3^2 \cong C_6^2 \oplus C_2$

Gruppo moltiplicativo $\mathbb{Z}/n\mathbb{Z}^*$

Se $n = \prod_{p \in \mathcal{P}} p^{n_p}$, per il teorema cinese del resto

$$\mathbb{Z}/n\mathbb{Z}^* \cong \prod_{p \in \mathcal{P}} \mathbb{Z}/p^{n_p}\mathbb{Z}^*.$$

Inoltre

1. $\mathbb{Z}/p^k\mathbb{Z}^* \cong C_{p^{k-1}(p-1)}$ se $p > 2$ è primo e $k > 0$.
2. $\mathbb{Z}/2^k\mathbb{Z}^* \cong C_{2^{k-2}} \times C_2$ se $k > 1$.

Se ne deduce che $\mathbb{Z}/n\mathbb{Z}^*$ è ciclico se e solo se

$$n = 1, 2, 4, p^k, 2p^k$$

con $p > 2$ primo e $k > 0$ (esercizio).

Dimostrazione di 2

Basta dimostrare che $\mathrm{ord}(\bar{5}) = 2^{k-2}$, perché poi $H := \langle\bar{5}\rangle$ e $K := \langle\overline{-1}\rangle = \{\bar{1}, \overline{-1}\}$ sono sottogruppi di $\mathbb{Z}/2^k\mathbb{Z}^*$ tali che $H \cap K = \{\bar{1}\}$ (perché $5^i \equiv 1 \not\equiv -1 \mod 4\ \forall\, i \in \mathbb{N}$), quindi

$$\#(HK) = (\#H)(\#K) = 2^{k-2} \cdot 2 = 2^{k-1} = \#\mathbb{Z}/2^k\mathbb{Z}^*,$$

e pertanto $\mathbb{Z}/2^k\mathbb{Z}^* = HK \cong H \times K \cong C_{2^{k-2}} \times C_2$.

Dimostriamo che $(\forall\, k \geq 2)\ 5^{2^{k-2}} = d_k 2^k + 1$ per qualche $d_k \in \mathbb{Z}$ tale che $2 \nmid d_k$. Per induzione su k: vero per $k = 2$ (con $d_2 = 1$); $k \implies k+1$ perché

$$5^{2^{k-1}} = (5^{2^{k-2}})^2 = (d_k 2^k + 1)^2 = d_k^2 2^{2k} + d_k 2^{k+1} + 1 = d_{k+1} 2^{k+1} + 1$$

con $d_{k+1} = d_k^2 2^{k-1} + d_k \equiv d_k \mod 2$ (dato che $k - 1 > 0$).

Dimostrazione di 1

Basta trovare $\bar{a}, \bar{b} \in \mathbb{Z}/p^k\mathbb{Z}^*$ (con $a, b \in \mathbb{Z}$ e $p \nmid a, b$) tali che $\operatorname{ord}(\bar{a}) = p - 1$ e $\operatorname{ord}(\bar{b}) = p^{k-1}$, perché poi $H := \langle \bar{a} \rangle$ e $K := \langle \bar{b} \rangle$ sono sottogruppi di $\mathbb{Z}/p^k\mathbb{Z}^*$ di ordini coprimi, quindi $H \cap K = \{\bar{1}\}$ e $\#(HK) = (\#H)(\#K) = (p-1)p^{k-1} = \#\mathbb{Z}/p^k\mathbb{Z}^*$, e pertanto $\mathbb{Z}/p^k\mathbb{Z}^* = HK \cong H \times K \cong C_{p-1} \times C_{p^{k-1}} \cong C_{p^{k-1}(p-1)}$.

- Preso $c \in \mathbb{Z}$ (con $p \nmid c$) tale che $\mathbb{Z}/p\mathbb{Z}^* = \langle c + p\mathbb{Z} \rangle$, si ha $\operatorname{ord}(\bar{c}) = m \operatorname{ord}(c + p\mathbb{Z}) = m(p-1)$ per qualche $m > 0$, quindi $\bar{a} := \bar{c}^m \in \mathbb{Z}/p^k\mathbb{Z}^*$ soddisfa $\operatorname{ord}(\bar{a}) = p - 1$.
- Posto $b := p + 1$ basta dimostrare che $b^{p^{k-1}} = d_k p^k + 1$ per qualche $d_k \in \mathbb{Z}$ tale che $p \nmid d_k$. Per induzione su k: vero per $k = 1$ (con $d_1 = 1$); $k \implies k + 1$ perché

$$b^{p^k} = (b^{p^{k-1}})^p = (d_k p^k + 1)^p = \sum_{i=0}^{p} \binom{p}{i} d_k^i p^{ki} = d_{k+1} p^{k+1} + 1$$

con $d_{k+1} = d_k + \sum_{i=2}^{p} \binom{p}{i} d_k^i p^{ki-k-1} \equiv d_k \mod p$ (dato che $p \mid \binom{p}{2}$ e $ki - k - 1 > 0$ se $i > 2$).