

4. IL LEMMA DI GAUSS

Lemma 4.1. (Gauss) $\text{Aut}(\mathbb{Z}_{p^m})$ con p primo dispari e $m \geq 1$ è ciclico.

Cominciamo a trattare il caso $m = 1$, caso in cui \mathbb{Z}_p è un campo. Per fare questo abbiamo bisogno di un lemma.

Lemma 4.2. Sia \mathbb{K} un campo. Allora

$$|\{x \in \mathbb{K} \mid x^d = 1\}| \leq d. \quad (1)$$

Proof. Osserviamo che un polinomio $p(x)$ di grado d a coefficienti in un campo \mathbb{K} ha al più d radici (vedo corso di Algebra 1). La (1) segue allora applicando questa osservazione al polinomio x^d . \square

Osservazione 4.3. Se si considera un polinomio su un anello che non sia un campo, può capitare che il numero di radici superi il grado del polinomio. Per esempio in \mathbb{Z}_{12} il polinomio $x^2 - 4$ ha tre radici: 2, 8, 10.

Lemma 4.4. (Lemma di Gauss per $m = 1$) $\text{Aut}(\mathbb{Z}_p)$ con p primo dispari è ciclico.

Proof. Dimostriamo che se \mathbb{K} è un campo e $G \leq \mathbb{K}^*$ un sottogruppo finito del gruppo moltiplicativo allora G è ciclico (da questo segue immediatamente che $\text{Aut}(\mathbb{Z}_p) \cong U(\mathbb{Z}_p) = (\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ è ciclico). Sia $k = \max\{o(a) \mid a \in G\}$ e sia $x \in G$ tale che $o(x) = k$. La dimostrazione sarà conclusa se dimostriamo che $|G| = k$ (infatti in questo caso $| \langle x \rangle | = |G| = k$). Mostriamo che $X = \{a \in G \mid a^k = 1\} = G$. Se per assurdo X fosse contenuto strettamente in G allora esisterebbe $y \in G$ tale che $y^k \neq 1$ e quindi $o(y) \nmid k$. Allora per un corollario precedente visto che x e z commutano (essendo G abeliano) esisterebbe $z \in G$ tale che

$$o(z) = [o(x), o(y)] = [k, o(y)] > k$$

che è la contraddizione cercata. Quindi $G = X$. Dal momento che $|G| \geq k$ e $|X| \leq k$ (per il Lemma 4.2) si deduce $|G| = k$. \square

Trattiamo ora il caso $m = 2$

Lemma 4.5. (Lemma di Gauss per $m = 2$) $\text{Aut}(\mathbb{Z}_{p^2})$ è ciclico.

Proof. Per il Lemma 4.4 esiste $[r]_p$ generatore di $\text{Aut}(\mathbb{Z}_p) = U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ e quindi $o([r]_p) = p-1$. Mostriamo che $[r]_{p^2}$ oppure $[r+p]_{p^2}$ generano $\text{Aut}(\mathbb{Z}_{p^2})$. Sia $x = o([r]_{p^2})$. Allora:

$$([r]_{p^2})^x = [r^x]_{p^2} = [1]_{p^2} \Rightarrow p^2 \mid (r^x - 1) \Rightarrow p \mid (r^x - 1) \Rightarrow [r]_p^x = [1]_p \Rightarrow x = s(p-1),$$

per un certo s naturale. Inoltre dal momento che $|\text{Aut}(\mathbb{Z}_{p^2})| = \Phi(p^2) = p(p-1)$ si ha

$$([r]_{p^2})^{p(p-1)} = [r^{p(p-1)}]_{p^2} = [1]_{p^2} \Rightarrow x = s(p-1) \mid p(p-1) \Rightarrow s \mid p \Rightarrow s = 1 \vee s = p$$

Quindi $x = p - 1$ oppure $x = p(p - 1)$. Analogamente se $y = o([r + p]_{p^2})$ allora $y = p - 1$ oppure $y = p(p - 1)$. Mostriamo che almeno uno tra x e y è uguale a $p(p - 1)$. Se per assurdo $x = y = p - 1$, allora, usando lo sviluppo del binomio di Newton si ha (compaiono solo i primi due termini in quando gli altri sono divisibili per p^2):

$$[1]_{p^2} = [r + p]_{p^2}^{p-1} = [r^{p-1} + (p-1)pr^{p-2}]_{p^2} = [1 + (p-1)pr^{p-2}]_{p^2} \neq [1]_{p^2}$$

(in quanto p non divide r (altrimenti $[r]_p = [0]_p$ e $[r]_p$ non sarebbe un generatore) e quindi $(p-1)r^{p-2}p$ non è divisibile per p^2) che è l'assurdo cercato. Visto che $|\text{Aut}(\mathbb{Z}_{p^2})| = p(p-1)$ segue che $\text{Aut}(\mathbb{Z}_{p^2})$ è generato da $[r]_{p^2}$ oppure da $[r + p]_{p^2}$ e quindi $\text{Aut}(\mathbb{Z}_{p^2})$ è ciclico. \square

Esempio 4.6. *Il generatore di $\text{Aut}(\mathbb{Z}_3) = \{[1]_3, [2]_3\} \cong \mathbb{Z}_2$ è $[2]_3$. I generatori di $\text{Aut}(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\} \cong \mathbb{Z}_6$ sono $[2]_9$ e $[5]_9$. Osserviamo che $[8]_9 = [5 + 3]_9$ non è un generatore in quanto $[8]_9^2 = [1]_9$.*

Prima di dimostrare il Lemma di Gauss in generale abbiamo bisogno dei seguenti due lemmi.

Lemma 4.7. *Siano $k \in \mathbb{Z}$ e p un primo dispari. Allora per ogni naturale $a \geq 1$ si ha*

$$([1 + kp]_{p^{a+2}})^{p^a} = [1 + kp^{a+1}]_{p^{a+2}} \quad (2)$$

Proof. La (2) è equivalente all'esistenza di $m_a \in \mathbb{Z}$ tale che

$$(1 + kp)^{p^a} = 1 + kp^{a+1} + m_a p^{a+2}, \quad (3)$$

per ogni $a \geq 1$.

Dimostriamo quindi la (3) per induzione su a . Se $a = 1$ allora

$$(1 + kp)^p = \sum_{j=0}^p \binom{p}{j} k^j p^j = 1 + kp^2 + k^2 \binom{p}{2} p^2 + p^3 \sum_{j=3}^p \binom{p}{j} k^j p^{j-3}.$$

Siccome $p \neq 2$ e p è primo allora $p \mid \binom{p}{2}$ e quindi $k^2 \binom{p}{2} p^2 = n_1 p^3$ per un certo naturale n_1 . Segue che

$$(1 + kp)^p = 1 + kp^2 + m_1 p^3.$$

con $m_1 = n_1 + \sum_{j=3}^p \binom{p}{j} k^j p^{j-3}$.

Supponiamo che la (3) sia vera e dimostriamola per $a + 1$. Allora

$$(1 + kp)^{p^{a+1}} = [(1 + kp)^{p^a}]^p = (1 + kp^{a+1} + m_a p^{a+2})^p = \sum_{i=0}^p \binom{p}{i} (1 + kp^{a+1})^{p-i} m_a^i p^{i(a+2)}. \quad (4)$$

Osserviamo che per $i \geq 1$ tutti i termini della somma precedente sono divisibili per p^{a+3} (infatti per $i = 1$ compare il termine $\binom{p}{1} p^{a+2} = p^{a+3}$, mentre per $i \geq 2$

compare il termine $p^{i(a+2)}$ che é sempre divisibile per p^{a+3} essendo $a \geq 1$. Quindi esiste $n_a \in \mathbb{Z}$ tale che

$$\sum_{i=1}^p \binom{p}{i} (1 + kp^{a+1})^{p-i} m_a^i p^{i(a+2)} = n_a p^{a+3}. \quad (5)$$

Osserviamo che il termine in (4) per $i = 0$ si scrive come

$$(1 + kp^{a+1})^p = \sum_{j=0}^p \binom{p}{j} k^j p^{j(a+1)} = 1 + kp^{a+2} + \sum_{j=2}^p \binom{p}{j} k^j p^{j(a+1)} \quad (6)$$

e $p^{a+3} | p^{ja+j}$ per ogni $j \geq 2$. Esiste quindi $n'_a \in \mathbb{Z}$ tale che

$$\sum_{j=2}^p \binom{p}{j} k^j p^{j(a+1)} = n'_a p^{a+3}. \quad (7)$$

Mettendo insieme la (5), la (6) e la (7) e ponendo $m_{a+1} = n_a + n'_a$ possiamo scrivere la (4) come

$$(1 + kp)^{p^{a+1}} = 1 + kp^{a+2} + m_{a+1} p^{a+3}$$

che é quello che volevamo dimostrare. \square

Osservazione 4.8. Nel corso della dimostrazione del Lemma 4.7 abbiamo usato l'ipotesi che p fosse un primo dispari solo solo nell'ipotesi induttiva.

Lemma 4.9. *Sia p un primo (non necessariamente dispari). Se $\text{Aut}(\mathbb{Z}_{p^m})$ é ciclico e $[r]_{p^m}$ é un suo generatore allora $[r]_{p^{m-1}}$ é un generatore di $\text{Aut}(\mathbb{Z}_{p^{m-1}})$. Se $[r]_{p^2}$ é un generatore di $\text{Aut}(\mathbb{Z}_{p^2})$ allora*

$$r^{p-1} = 1 + kp \quad (8)$$

per qualche intero k tale che $p \nmid k$.

Proof. L'applicazione

$$\text{Aut}(\mathbb{Z}_{p^m}) = U(\mathbb{Z}_{p^m}) \rightarrow \text{Aut}(\mathbb{Z}_{p^{m-1}}) = U(\mathbb{Z}_{p^{m-1}}), [u]_{p^m} \mapsto [u]_{p^{m-1}}$$

è un omomorfismo suriettivo di gruppi e quindi se $\text{Aut}(\mathbb{Z}_{p^m})$ é ciclico allora $\text{Aut}(\mathbb{Z}_{p^{m-1}})$ é ciclico e se $[r]_{p^m}$ é un generatore di $\text{Aut}(\mathbb{Z}_{p^m})$ allora $[r]_{p^{m-1}}$ é un generatore di $\text{Aut}(\mathbb{Z}_{p^{m-1}})$. Se, in particolare, $[r]_{p^2}$ é un generatore di $\text{Aut}(\mathbb{Z}_{p^2})$ allora $[r]_p$ é un generatore di $\text{Aut}(\mathbb{Z}_p)$ e quindi $([r]_p)^{p-1} = [1]_p$ ossia $r^{p-1} = 1 + kp$, per qualche intero k . Inoltre $p \nmid k$ altrimenti $[r]_{p^2}^{p-1} = [1]_{p^2}$ in contrasto col fatto che $[r]_{p^2}$ genera $\text{Aut}(\mathbb{Z}_{p^2})$ e quindi ha ordine $p(p-1)$. \square

Dimostrazione del Lemma di Gauss (Lemma 4.1) Sia p un primo dispari. Dimostriamo che $\text{Aut}(\mathbb{Z}_{p^m})$ è ciclico per ogni $m \geq 3$. Sia $[r]_{p^2}$ un generatore di $\text{Aut}(\mathbb{Z}_{p^2})$ la cui esistenza è garantita dal Lemma 4.5. Sia $x = o([r]_{p^m})$. Allora:

$$([r]_{p^m})^x = [r^x]_{p^m} = [1]_{p^m} \Rightarrow p^m | (r^x - 1) \Rightarrow p | (r^x - 1) \Rightarrow [r^x]_p = [1]_p \Rightarrow x = s(p-1),$$

per un certo $s \in \mathbb{N}_+$. Inoltre

$$[r^{p^{m-1}(p-1)}]_{p^m} = [1]_{p^m} \Rightarrow x = s(p-1) \mid p^{m-1}(p-1),$$

Allora $x = p^a(p-1)$ dove $a = 0, \dots, m-1$. La dimostrazione sarà conclusa se si dimostra che $x = p^{m-1}(p-1)$ (infatti in questo caso $[r]_{p^m}$ un generatore di $\text{Aut}(\mathbb{Z}_{p^m})$ che ha cardinalità $p^{m-1}(p-1)$). Supponiamo per assurdo che $x = p^b(p-1)$, $b = 0, \dots, m-2$. Allora, in particolare,

$$([r]_{p^m})^{p^{m-2}(p-1)} = [1]_{p^m}.$$

Segue che

$$[1]_{p^m} = ([r]_{p^m})^{p^{m-2}(p-1)} = ([r^{p-1}]_{p^m})^{p^{m-2}} = ([1+kp]_{p^m})^{p^{m-2}} = [1+kp^{m-1}]_{p^m}$$

dove nell'ultima uguaglianza abbiamo usato la (2) del Lemma 4.7 con $m = a + 2$. D'altra parte $[1+kp^{m-1}]_{p^m} \neq [1]_{p^m}$ in quanto $p \nmid k$. Questo é l'assurdo desiderato e la dimostrazione é conclusa. \square

5. IL TEOREMA DI GAUSS

Teorema 5.1. (*Gauss*) $\text{Aut}(\mathbb{Z}_n)$ é ciclico se e solo se $n \in \{1, 2, 4, p^m, 2p^m\}$ con p primo dispari.

Proof. Iniziamo a dimostrare che se $n \in \{1, 2, 4, p^m, 2p^m\}$ (con p primo dispari) allora \mathbb{Z}_n é ciclico. Per $n = 1$ e $n = 2$ otteniamo rispettivamente il gruppo banale e \mathbb{Z}_2 che hanno entrambi come gruppo di automorfismi il gruppo banale; per $n = 4$, $\text{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$; il caso $n = p^m$ é il Lemma di Gauss. Infine se $n = 2p^m$ allora $\mathbb{Z}_n \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^m}$ da cui (essendo $(2, p^m) = 1$)

$$\text{Aut}(\mathbb{Z}_n) \cong \text{Aut}(\mathbb{Z}_2) \times \text{Aut}(\mathbb{Z}_{p^m}) \cong \{0\} \times \text{Aut}(\mathbb{Z}_{p^m}) \cong \text{Aut}(\mathbb{Z}_{p^m})$$

il quale é ciclico ancora per il Lemma di Gauss.

Mostriamo ora che se $\text{Aut}(\mathbb{Z}_n)$ é ciclico allora $n \in \{1, 2, 4, p^m, 2p^m\}$ (con p primo dispari).

Scriviamo

$$n = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}, \quad \alpha_j \geq 0, \quad p_i \neq p_j,$$

dove i p_i sono primi dispari distinti.

Iniziamo a dimostrare che esiste al massimo un primo dispari in questa scomposizione. Supponiamo per assurdo che esistano due primi dispari distinti. Possiamo supporre siano p_1 e p_2 e quindi $\alpha_1 \geq 1$ e $\alpha_2 \geq 1$. Allora $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \mathbb{Z}_r$, dove $r = 2^{\alpha_0} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$ e quindi $\text{Aut}(\mathbb{Z}_n) \cong \text{Aut}(\mathbb{Z}_{p_1^{\alpha_1}}) \times \text{Aut}(\mathbb{Z}_{p_2^{\alpha_2}}) \times \text{Aut}(\mathbb{Z}_r)$ (per il teorema sul prodotto diretto di gruppi con cardinalità coprime). Essendo $\text{Aut}(\mathbb{Z}_n)$ ciclico segue che $\text{Aut}(\mathbb{Z}_{p_1^{\alpha_1}})$ e $\text{Aut}(\mathbb{Z}_{p_2^{\alpha_2}})$ sono gruppi ciclici e i loro ordini sono primi

tra loro. Ma

$$|\text{Aut}(\mathbb{Z}_{p_i^{\alpha_i}})| = \Phi(p_i^{\alpha_i}) = p_i^{\alpha_i-1}(p_i - 1)$$

sono pari per $i = 1, 2$, che é l'assurdo cercato. Quindi $n = 2^{\alpha_0}p^\alpha$ con p primo dispari. Dobbiamo quindi dimostrare che $\text{Aut}(\mathbb{Z}_n)$ non é ciclico nei due casi $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$ e $n = 2^{\alpha_0}p^\alpha$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$.

Consideriamo il primo caso, $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$. Se per assurdo $\text{Aut}(\mathbb{Z}_{2^{\alpha_0}})$, con $\alpha_0 \geq 3$ fosse ciclico allora, per il Lemma 4.9, $\text{Aut}(\mathbb{Z}_8)$ sarebbe ciclico in contrasto col fatto che $\text{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Infine mostriamo che $\text{Aut}(\mathbb{Z}_n)$ non é ciclico se $n = 2^{\alpha_0}p^\alpha$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$. Dall'isomorfismo $\mathbb{Z}_m \cong \mathbb{Z}_{2^{\alpha_0}} \times \mathbb{Z}_{p^\alpha}$ si ottiene $\text{Aut}(\mathbb{Z}_n) \cong \text{Aut}(\mathbb{Z}_{2^{\alpha_0}}) \times \text{Aut}(\mathbb{Z}_{p^\alpha})$ (sempre per il teorema sul prodotto diretto di gruppi con cardinalità coprime). Ma le cardinalità di $|\text{Aut}(\mathbb{Z}_{2^{\alpha_0}})| = \Phi(2^{\alpha_0}) = 2^{\alpha_0-1}$ e $|\text{Aut}(\mathbb{Z}_{p^\alpha})| = p^{\alpha-1}(p-1)$ che sono entrambe pari ($\alpha_0 \geq 2$ e p primo dispari). Quindi $\text{Aut}(\mathbb{Z}_n)$ non é ciclico, che é la contraddizione cercata. \square