7.4 Il Lemma e il Teorema di Gauss

Lemma 7.4.1 *(Gauss) Il gruppo Aut$(\mathbb{Z}_{p^m})$ è ciclico per ogni primo dispari p e per ogni $m \geq 1$.*

Dimostriamo solo il caso $m = 1$, in cui $\mathbb{Z}_p$ è un campo. Il lettore interessato al caso generale potrà consultare l'Appendice A.

Lemma 7.4.2 *(Lemma di Gauss per $m = 1$) Aut$(\mathbb{Z}_p)$, con p primo dispari, è ciclico.*

Dimostrazione: Dimostriamo che se $\mathbb{K}$ è un campo e $G \leq \mathbb{K}^*$ è un sottogruppo finito del gruppo moltiplicativo, allora G è ciclico (da ciò segue immediatamente che $\mathrm{Aut}(\mathbb{Z}_p) \cong U(\mathbb{Z}_p) = (\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ 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 $|G| = k$.

Consideriamo

$$X = \{a \in G \mid a^k = 1\} \subseteq G.$$

Se per assurdo $X \neq G$, allora esisterebbe $y \in G$ tale che $y^k \neq 1$, e quindi $o(y) \nmid k$. Per il Corollario 3.5.14, poiché x e y commutano (essendo G abeliano), esisterebbe $z \in G$ tale che $o(z) = [o(x), o(y)] = [k, o(y)] > k$, contraddicendo l'ipotesi.

Quindi $G = X$. Dato che $k = |\langle\, x \,\rangle| \leq |G|$ e $|X| \leq k$, in quanto il polinomio $x^k - 1$ (a coefficienti nel campo $\mathbb{K}$) ha al più k radici, si conclude che $|G| = k$. $\square$

Teorema 7.4.3 (Gauss) *Il gruppo Aut$(\mathbb{Z}_n)$ è ciclico se e solo se $n \in \{1, 2, 4, p^m, 2p^m\}$, con p un primo dispari.*

Dimostrazione: Iniziamo dimostrando che se $n \in \{1, 2, 4, p^m, 2p^m\}$, con p primo dispari, allora $\mathrm{Aut}(\mathbb{Z}_n)$ è ciclico.

Per i casi $n = 1$ e $n = 2$, abbiamo rispettivamente il gruppo banale e $\mathbb{Z}_2$, i cui gruppi di automorfismi sono entrambi banali. Per $n = 4$, si ha $\mathrm{Aut}(\mathbb{Z}_4) = \mathbb{Z}_2$. Il caso $n = p^m$ segue dal Lemma di Gauss (Lemma 7.4.1). Infine, se $n = 2p^m$, allora poiché $(2, p^m) = 1$, sia ha $\mathbb{Z}_n \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^m}$ e per il Teorema 6.3.1

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

che è ciclico, ancora per il Lemma di Gauss.

Mostriamo ora che se $\mathrm{Aut}(\mathbb{Z}_n)$ è 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.

Dimostriamo che può esserci al massimo un solo primo dispari nella scomposizione di n. Supponiamo per assurdo che esistano due primi dispari distinti, diciamo p_1 e p_2, con $\alpha_1 \geq 1$ e $\alpha_2 \geq 1$. In questo caso, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \mathbb{Z}_r$, dove $r = 2^{\alpha_0} p_3^{\alpha_3} \cdots p_t^{\alpha_t}$. Allora, per il Teorema 6.3.1, si ha

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}}) \times \mathrm{Aut}(\mathbb{Z}_{p_2^{\alpha_2}}) \times \mathrm{Aut}(\mathbb{Z}_r).$$

Essendo $\mathrm{Aut}(\mathbb{Z}_n)$ ciclico, anche $\mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}})$ e $\mathrm{Aut}(\mathbb{Z}_{p_2^{\alpha_2}})$ devono essere ciclici, e i loro ordini devono essere primi tra loro. Tuttavia,

$$|\mathrm{Aut}(\mathbb{Z}_{p_i^{\alpha_i}})| = \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1),$$

che è pari per $i = 1, 2$, portando così a una contraddizione. Quindi, $n = 2^{\alpha_0} p^{\alpha}$, con p un primo dispari.

Restano ora da esaminare i casi $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$ e $n = 2^{\alpha_0} p^{\alpha}$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$, per mostrare che in questi casi $\mathrm{Aut}(\mathbb{Z}_n)$ non è ciclico.

Consideriamo innanzitutto il caso $n = 2^{\alpha_0}$ con $\alpha_0 \geq 3$. Supponiamo, per assurdo che $\mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}})$ sia ciclico. Consideriamo l'applicazione

$$\mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}}) = U(\mathbb{Z}_{2_0^{\alpha}}) \to \mathrm{Aut}(\mathbb{Z}_8) = U(\mathbb{Z}_8), [u]_{2^{\alpha_0}} \mapsto [u]_8$$

che è un omomorfismo suriettivo di gruppi e quindi $\mathrm{Aut}(\mathbb{Z}_8)$ dovrebbe essere ciclico, ma $\mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, non è ciclico.

Infine, consideriamo il caso $n = 2^{\alpha_0} p^{\alpha}$ con $\alpha_0 \geq 2$ e $\alpha \geq 1$. Dall'isomorfismo $\mathbb{Z}_n \cong \mathbb{Z}_{2^{\alpha_0}} \times \mathbb{Z}_{p^{\alpha}}$, si ottiene

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}}) \times \mathrm{Aut}(\mathbb{Z}_{p^{\alpha}}),$$

nuovamente per il Teorema 6.3.1. Tuttavia, le cardinalità sono

$$|\mathrm{Aut}(\mathbb{Z}_{2^{\alpha_0}})| = \varphi(2^{\alpha_0}) = 2^{\alpha_0 - 1}, \quad |\mathrm{Aut}(\mathbb{Z}_{p^{\alpha}})| = p^{\alpha - 1}(p - 1),$$

entrambe pari (poiché $\alpha_0 \geq 2$ e p è un primo dispari), il che implica che $\mathrm{Aut}(\mathbb{Z}_n)$ non è ciclico, ottenendo così la contraddizione cercata. $\square$