Appendice A

Lemma 7.5.1 *(Lemma di Gauss per $m = 2$) $Aut(\mathbb{Z}_{p^2})$ è ciclico.*

Dimostrazione: Dal Lemma 7.4.2, esiste $[r]_p$, generatore di $\mathrm{Aut}(\mathbb{Z}_p) = U(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, con $o([r]_p) = p - 1$. Mostriamo che sia $[r]_{p^2}$ sia $[r+p]_{p^2}$ generano $\mathrm{Aut}(\mathbb{Z}_{p^2})$.

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 $s \in \mathbb{N}$.

Inoltre, poiché $|\,\mathrm{Aut}(\mathbb{Z}_{p^2})| = \varphi(p^2) = p(p-1)$, si ha:

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

dove $x = p^a(p-1)$ con $a = 0, \ldots, m-1$. Dimostreremo ora che $x = p^{m-1}(p-1)$.

Supponiamo per assurdo che $x = p^b(p-1)$ con $b = 0, \ldots, m-2$. Allora:

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

Ne consegue che:

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

dove abbiamo usato il Lemma 7.5.3 per ottenere l'ultima uguaglianza. Tuttavia, $[1+kp^{m-1}]_{p^2} \neq [1]_{p^2}$, poiché $p \nmid k$. Questa è l'assurdo che cercavamo.

Poiché $|\,\mathrm{Aut}(\mathbb{Z}_{p^2})| = p(p-1)$, segue che $\mathrm{Aut}(\mathbb{Z}_{p^2})$ è generato da $[r]_{p^2}$ o $[r+p]_{p^2}$ e quindi è ciclico. $\square$

Esempio 7.5.2 Il generatore di $\mathrm{Aut}(\mathbb{Z}_3) = \{[1]_3, [2]_3\} \cong \mathbb{Z}_2$ è $[2]_3$. I generatori di $\mathrm{Aut}(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\} \cong \mathbb{Z}_6$ sono $[2]_9$ e $[5]_9$. Osserviamo che $[8]_9 = [5+3]_9$ non è un generatore, poiché $[8]_9^2 = [1]_9$.

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

Lemma 7.5.3 *Siano $k \in \mathbb{Z}$ e p un primo dispari. Allora per ogni naturale $a \geq 1$ si ha*

$$\left([1+kp]_{p^{a+2}}\right)^{p^a} = [1+kp^{a+1}]_{p^{a+2}} \tag{7.2}$$

Dimostrazione: La (7.2) é equivalente all'esistenza di $m_a \in \mathbb{Z}$ tale che

$$(1+kp)^{p^a} = 1+kp^{a+1}+m_a p^{a+2}, \tag{7.3}$$

per ogni $a \geq 1$.

Dimostriamo quindi la (7.3) 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 é primo allora $p|\binom{p}{2}$ e quindi $k^2\binom{p}{2}p^2 = n_1 p^3$ per un certo naturale n_1. Segue che

$$(1+kp)^p = 1+kp^2+m_1p^3.$$

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

Supponiamo che la (7.3) sia vera e dimostriamola per $a+1$. Allora

$$(1+kp)^{p^{a+1}} = [(1+kp)^{p^a}]^p = (1+kp^{a+1}+m_a p^{a+2})^p = \sum_{i=0}^{p}\binom{p}{i}(1+kp^{a+1})^{p-i}m_a^i p^{i(a+2)}. \tag{7.4}$$

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 divsibile per p^{a+3} essendo $a \geq 1$. Quindi esiste $n_a \in \mathbb{Z}$ tale che

$$\sum_{i=1}^{p}\binom{p}{i}(1+kp^{a+1})^{p-i}m_a^i p^{i(a+2)} = n_a p^{a+3}. \tag{7.5}$$

Osserviamo che il termine in (7.4) per $i=0$ si scrive come

$$(1+kp^{a+1})^p = \sum_{j=0}^{p}\binom{p}{j}k^j p^{j(a+1)} = 1+kp^{a+2}+\sum_{j=2}^{p}\binom{p}{j}k^j p^{j(a+1)} \tag{7.6}$$

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

$$\sum_{j=2}^{p}\binom{p}{j}k^j p^{j(a+1)} = n'_a p^{a+3}. \tag{7.7}$$

Mettendo insieme la (7.5), la (7.6) e la (7.7) e ponendo $m_{a+1} = n_a + n'_a$ possiamo scrivere la (7.4) come

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

che é quello che volevamo dimostrare. □

Osservazione 7.5.4 Nel corso della dimostrazione del Lemma 7.5.3 abbiamo usato l'ipotesi che p fosse un primo dispari solo solo nell'ipotesi induttiva.

Lemma 7.5.5 *Sia p un primo (non necessariamente dispari). Se $Aut(\mathbb{Z}_{p^m})$ é ciclico e $[r]_{p^m}$ é un suo generatore allora $[r]_{p^{m-1}}$ é un generatore di $Aut(\mathbb{Z}_{p^{m-1}})$. Se $[r]_{p^2}$ é un generatore di $Aut(\mathbb{Z}_{p^2})$ allora*

$$r^{p-1} = 1 + kp \tag{7.8}$$

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

Dimostrazione: L'applicazione

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

è un omomorfismo suriettivo di gruppi e quindi se $\mathrm{Aut}(\mathbb{Z}_{p^m})$ é ciclico allora $\mathrm{Aut}(\mathbb{Z}_{p^{m-1}})$ é ciclico e se $[r]_{p^m}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^m})$ allora generatore $[r]_{p^{m-1}}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^{m-1}})$. Se, in particolare, $[r]_{p^2}$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^2})$ allora $[r]_p$ é un generatore di $\mathrm{Aut}(\mathbb{Z}_p)$ 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 $\mathrm{Aut}(\mathbb{Z}_{p^2})$ e quindi ha ordine $p(p-1)$. □

Dimostrazione del Lemma di Gauss (Lemma 7.4.1) Sia p un primo dispari. Dimostriamo che $\mathrm{Aut}(\mathbb{Z}_{p^m})$ è ciclico per ogni $m \geq 3$. Sia $[r]_{p^2}$ un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^2})$ la cui esistenza è garantita dal Lemma 7.5.1. 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 $a = 0, \ldots, m-1$. La dimostrazione sará conclusa se si dimostra che $x = p^{m-1}(p-1)$ (infatti in questo caso $[r]_{p^m}$ un generatore di $\mathrm{Aut}(\mathbb{Z}_{p^m})$ che ha cardinalitá $p^{m-1}(p-1)$). Supponiamo per assurdo che $x = p^b(p-1)$, $b = 0, \ldots, m-2$. 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 (7.2) del Lemma 7.5.3 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. $\square$