Esercizi per algebra 2

Francesco Genovese

28 marzo 2014

1 Polinomi ciclotomici di potenze di un primo

Dato un primo p e un intero $n \geq 1$, mostriamo che il polinomio

$$F(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}$$

è irriducibile in $\mathbb{Z}[X]$. Iniziamo scrivendo

$$\begin{aligned} F(X) &= \frac{(X^{p^{n-1}})^p - 1}{X^{p^{n-1}} - 1} = \frac{(X^{p^{n-1}} - 1)((X^{p^{n-1}})^{p-1} + (X^{p^{n-1}})^{p-2} \cdots + 1)}{X^{p^{n-1}} - 1} \\ &= (X^{p^{n-1}})^{p-1} + (X^{p^{n-1}})^{p-2} + \cdots + 1. \end{aligned}$$

Sappiamo che $F(X)$ è irriducibile se e solo se il traslato $F(X+1)$ è irriducibile. L'idea è quella di applicare il criterio di Eisenstein proprio a $F(X+1)$. Abbiamo:

$$F(X+1) = ((X+1)^{p^{n-1}})^{p-1} + ((X+1)^{p^{n-1}})^{p-2} + \cdots + 1$$

Per vedere se Eisenstein è applicabile, consideriamo la riduzione modulo p di $F(X+1)$. Il vantaggio della riduzione è che

$$(X+1)^{p^{n-1}} \equiv X^{p^{n-1}} + 1$$

come polinomi in $\mathbb{F}_p[X]$ (lo si vede direttamente applicando la formula binomiale). Dunque, possiamo scrivere:

$$F(X+1) \equiv \frac{(X^{p^{n-1}} + 1)^p - 1}{(X^{p^{n-1}} + 1) - 1} \equiv \frac{X^{p^n}}{X^{p^{n-1}}} \equiv X^{(p-1)p^{n-1}},$$

come polinomio in $\mathbb{F}_p[X]$. Questo significa che il primo p non divide il coefficiente di grado massimo di $F(X+1)$ e divide tutti gli altri coefficienti. Per finire, uno si accorge (abbastanza direttamente) che il termine noto è proprio p, e dunque p^2 non lo divide. L'irriducibilità di $F(X+1)$ in $\mathbb{Z}[X]$ segue dunque dal criterio di Eisenstein.

2 Esercizio: il polinomio $X^4 - 3X + 2$

Dato il polinomio $q(X) = X^4 - 3X + 2 \in \mathbb{Q}[X]$, trovare un campo di spezzamento K, determinare il grado $[K : \mathbb{Q}]$, e trovare γ tale che $K = \mathbb{Q}(\gamma)$.

Notiamo subito che 2 è radice di $q(X)$. Dividiamo per $X - 2$, trovando la fattorizzazione:

$$q(X) = (X - 2)(X^3 + X^2 + X - 2).$$

Dunque, possiamo ridurci a cercare un campo di spezzamento del polinomio

$$p(X) = X^3 + X^2 + X - 2.$$

$p(X)$ è irriducibile sui razionali: infatti, se fosse riducibile, dovrebbe avere una radice che divide il termine noto, ossia ± 1 o ± 2, ma un'ispezione diretta ci mostra che nessuna di queste annulla p. Osserviamo che $p(X)$ ammette una sola radice reale. Infatti, vedendolo come funzione $\mathbb{R} \to \mathbb{R}$, la sua derivata

$$p'(X) = 3X^2 + 2X + 1$$

è un polinomio di secondo grado con discriminante negativo, dunque è strettamente positiva, cioè p è crescente vista come funzione $\mathbb{R} \to \mathbb{R}$, ed è quindi forzata ad avere un'unica radice reale.

Sia $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ l'unica radice reale di $p(X)$. Dividiamo per $X - \alpha$, e troviamo la fattorizzazione:

$$p(X) = (X - \alpha)(X^2 + (1 + \alpha)X + 1 + \alpha + \alpha^2).$$

Troviamo le altre radici di p, ossia le radici di $r(X) = X^2 + (1 + \alpha)X + 1 + \alpha + \alpha^2$, che è un polinomio in $\mathbb{Q}(\alpha)$. Il discriminante di questo polinomio è

$$\Delta = \alpha^2 + 2\alpha + 1 - 4 - 4\alpha - 4\alpha^2 = -3\alpha^2 - 2\alpha - 3.$$

Notiamo che $\Delta < 0$, questo perché il polinomio $3X^2 + 2X + 3$ ha discriminante negativo, dunque assume valori sempre strettamente positivi. Poniamo $D = -\Delta = 3\alpha^2 + 2\alpha + 3 > 0$. Allora, le radici di $r(X)$ sono:

$$\omega = \frac{-1 - \alpha + i\sqrt{D}}{2},$$
$$\overline{\omega} = \frac{-1 - \alpha - i\sqrt{D}}{2}.$$

A questo punto, un campo di spezzamento di p su $\mathbb{Q}$ è dato da $\mathbb{Q}(\alpha, \omega)$: infatti, $\omega + \overline{\omega} = -1 - \alpha$, dunque $\overline{\omega} \in \mathbb{Q}(\alpha, \omega)$ (del resto, $\overline{\omega}$ è la complessa coniugata di ω).

Calcoliamo il grado dell'estensione $\mathbb{Q}(\alpha, \omega)$ su $\mathbb{Q}$. Usiamo la transitività dei gradi:

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Il polinomio minimo di α su $\mathbb{Q}$ è p: $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$; il polinomio minimo di ω su $\mathbb{Q}(\alpha)$ è r, giacché $\omega \notin \mathbb{Q}(\alpha)$ perché non è un numero reale, dunque $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = 2$. Concludiamo che $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$.

Cerchiamo ora un elemento primitivo dell'estensione. Per cominciare, osserviamo che $\alpha + 2\omega + 1 = i\sqrt{D}$, e dunque $\mathbb{Q}(\alpha + 2\omega) = \mathbb{Q}(i\sqrt{D})$. Proviamo a mostrare che $\alpha \in \mathbb{Q}(i\sqrt{D})$; a quel punto, allora, seguirà che $2\omega \in \mathbb{Q}(i\sqrt{D})$ (poiché $\alpha + 2\omega \in \mathbb{Q}(i\sqrt{D})$), da cui $\omega \in \mathbb{Q}(i\sqrt{D})$, e dunque $\mathbb{Q}(\alpha, \omega) \subseteq \mathbb{Q}(i\sqrt{D}) = \mathbb{Q}(\alpha + 2\omega) \subseteq \mathbb{Q}(\alpha, \omega)$. Alla fine avremo ottenuto che

$$\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha + 2\omega) = \mathbb{Q}(i\sqrt{D}),$$

come volevamo.

Dimostriamo addirittura che $\alpha \in \mathbb{Q}(3\alpha^2 + 2\alpha) = \mathbb{Q}(3\alpha^2 + 2\alpha + 3) = \mathbb{Q}(D) \subset \mathbb{Q}(i\sqrt{D})$. Questa affermazione è equivalente a $\mathbb{Q}(\alpha) = \mathbb{Q}(3\alpha^2 + 2\alpha)$ (l'inclusione $\mathbb{Q}(3\alpha^2 + 2\alpha) \subseteq \mathbb{Q}(\alpha)$ è banale). Consideriamo le estensioni $\mathbb{Q} \subseteq \mathbb{Q}(3\alpha^2 + 2\alpha) \subseteq \mathbb{Q}(\alpha)$. La transitività dei gradi ci dice che

$$3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(3\alpha^2 + 2\alpha)][\mathbb{Q}(3\alpha^2 + 2\alpha) : \mathbb{Q}].$$

Abbiamo solo due possibilità:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(3\alpha^2 + 2\alpha)] = 1, \quad [\mathbb{Q}(3\alpha^2 + 2\alpha) : \mathbb{Q}] = 3$$

oppure

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(3\alpha^2 + 2\alpha)] = 3, \quad [\mathbb{Q}(3\alpha^2 + 2\alpha) : \mathbb{Q}] = 1.$$

La seconda possibilità, però, è impossibile! Infatti, se $[\mathbb{Q}(3\alpha^2 + 2\alpha) : \mathbb{Q}] = 1$, dovremmo avere che $3\alpha^2 + 2\alpha \in \mathbb{Q}$, e in particolare α sarebbe radice di un polinomio di secondo grado a coefficienti in $\mathbb{Q}$, ma questo è impossibile, perché il polinomio minimo di α su $\mathbb{Q}$ ha grado 3! Dunque, deve essere vera la prima possibilità, in particolare $[\mathbb{Q}(\alpha) : \mathbb{Q}(3\alpha^2 + 2\alpha)] = 1$, da cui necessariamente $\mathbb{Q}(\alpha) = \mathbb{Q}(3\alpha^2 + 2\alpha)$, e possiamo concludere.