Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2021/2022
AL310 - Istituzioni di Algebra Superiore
I Esercitazione - 9 marzo 2022

Richiami sulla fattorizzazione

Sia A un UFD ed indichiamo con $A[x]$ il corrispondente anello di polinomi a coefficienti in A. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ un polinomio di grado $n \geq 1$ (i.e. $a_n \neq 0$) che, per semplicità, assumeremo primitivo (i.e. $\gcd(a_0, a_1, \ldots, a_n) = 1$).

1. $\alpha \in A$ è una radice di $f(x)$ sse $x - \alpha$ divide $f(x)$ in $A[x]$.

2. Un elemento $\alpha \in A$ è irriducibile in $A[x]$ sse è irriducibile in A.

3. Gli elementi invertibili di $A[x]$ sono gli elementi invertibili di A.

4. $A[x]$ è un UFD.

5. (Gauss) Sia $Q_Z(A)$ il campo dei quozienti di A. $f(x)$ è irriducibile in $A[x]$ sse è irriducibile in $Q_Z(A)[x]$.

6. (Eisenstein) Se esiste un primo $p \in A$ tale che p divide $a_0, a_1, \ldots, a_{n-1}$, p non divide a_n e p^2 non divide a_0, allora $f(x)$ è irriducibile in $A[x]$.

7. Se $f(x)$ è monico e ha grado 2 o 3, allora $f(x)$ è irriducibile in $A[x]$ sse non ha radici in A.

Caso $A = \mathbb{C}$

Dal teorema fondamentale dell'algebra si deduce che esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$, non necessariamente distinti, tali che

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Quindi in $\mathbb{C}[x]$ un polinomio è irriducibile sse ha grado 1.

Caso $A = \mathbb{R}$

Se $\alpha \in \mathbb{C} \setminus \mathbb{R}$ è una radice di $f(x)$, allora il polinomio reale $x^2 - 2\Re(\alpha)x + |\alpha|^2$ divide $f(x) \in \mathbb{R}[x]$. Ne segue che i polinomi irriducibili in $\mathbb{R}[x]$ sono costituiti dai polinomi di primo grado e da quelli di secondo grado senza radici reali.

Caso $A = \mathbb{Q}$

Si può sempre scrivere il polinomio nella forma$f(x) = cf_1(x)$ con c invertibile e $f_1(x) \in \mathbb{Z}[x]$ primitivo. In virtù di (5) l'irriducibilità di $f(x) \in \mathbb{Q}[x]$ 'e equivalente all'irreducibilità di $f_1(x)$ in $\mathbb{Z}[x]$.

Caso $A = \mathbb{Z}$

Per stabilre l'irriducibilità di $f(x)$ si possono utilizzare:

- il citato criterio di Eisenstein (e sue varianti: applicarlo a $f(x+c)$,$x^n f(1/x)$);

- la riduzione modulo p;

- la "forza bruta".

Richiami sugli anelli e sui campi

Sia $\mathbb{K}$ un campo. Dato $f(x) \in \mathbb{K}[x]$, denotiamo con $\mathbb{K}[x]/(f(x))$ l'anello ottenuto quozientando $\mathbb{K}[x]$ con l'ideale generato da $f(x)$.

1. Un elemento $g(x)+(f(x)) \in \mathbb{K}[x]/(f(x))$ è invertibile sse $\gcd(f(x),(g(x)) = 1$; in tal caso, se $1 = h_1(x)f(x) + h_2(x)g(x)$ è una corrispondente identità di Bézout, l'inverso di $g(x) + (f(x))$ è dato da $h_2(x) + (f(x))$.
2. $\mathbb{K}[x]/(f(x))$ è un campo sse $f(x)$ è irriducibile in $\mathbb{K}[x]$.
3. (Teorema cinese dei resti) Se $f(x) = f_1(x)f_2(x)\cdots f_n(x)$ in $\mathbb{K}[x]$ con $\gcd(f_i(x), f_j(x)) = 1$ per $i \neq j$, allora
$$\mathbb{K}[x]/(f(x)) \cong \mathbb{K}[x]/(f_1(x)) \times \mathbb{K}[x]/(f_2(x)) \times \cdots \times \mathbb{K}[x]/(f_n(x)).$$

Sia $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ un catena di estensioni di campi. Allora
$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}].$$

Esercizio 1. Sia$f(x) = x^4 - 5x^3 + x^2 + 1 \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$. Fattorizzare il polinomio ridotto modulo 2 $\overline{f}_2(x) \in \mathbb{Z}_2[x]$. Dedurne che $f(x)$ è irriducibile in $\mathbb{Q}[x]$ (e in $\mathbb{Z}[x]$).

Esercizio 2. Sia $f(x, y) = x^2+y^2+1 \in \mathbb{C}[x, y] = (\mathbb{C}[y])[x]$. Utilizzare il criterio di Eisenstein per mostrare che f è irriducibile in $\mathbb{C}[x, y]$.

Esercizio 3. Sia
$$\begin{array}{cccc} v\colon & \mathbb{R}[x] & \to & \mathbb{C} \\ & f(x) & \mapsto & f(i) \end{array}$$
Mostrare che v è un omomorfismo unitario di anelli. Determinare $\mathrm{Im}(v)$ e $\ker(v)$.

Esercizio 4. Senza utilizzare i risultati del precedente esercizio, trovare l'inverso di $ax + b + (x^2 + 1) \in \mathbb{R}[x]/(x^2 + 1)$ nel caso $a \neq 0$.

Esercizio 5. Sia $f(x) \in \mathbb{R}[x]$ monico e di grado positivo con radici tutte distinte (le radici possono essere anche complesse). Descrivere gli anelli $\frac{\mathbb{R}[x]}{(f(x))}$ e $\frac{\mathbb{C}[x]}{(f(x))}$. Cosa accade abolendo l'ipotesi sulla semplicità delle radici del polinomio?

Esercizio 6. Trovare il $\gcd(x^5 + x^2 + x + 1, x^2 + x)$ ed una corrispondente identità di Bézout.

Esercizio 7. Al variare di $n \in \mathbb{N}^*$, si consideri l'insieme $C_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

(i) Dimostrare che C_n è un sottogruppo di $\mathbb{C}^*$.

(ii) Provare che C_n è ciclico e quindi isomorfo a $\mathbb{Z}_n$ ed individuare i suoi generatori.

(iii) Dimostrare che se $n \mid m$ allora $C_n \subseteq C_m$.

(iv) Siano $m, n \geq 1$ interi distinti. Dire se $C_m \cup C_n = C_{mn}$.

Esercizio 8. Sia $\mathbb{F} \subseteq \mathbb{E}$ un ampliamento di campi. Siano α, $\beta \in \mathbb{E}$ algebrici su $\mathbb{F}$ di gradi rispettivamente m ed n, tali che $\gcd(m, n) = 1$.

Provare che:

(i) $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = mn$;

(ii) $\mathbb{F}(\alpha) \cap \mathbb{F}(\beta) = \mathbb{F}$