TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 10

Esercizio 10.1. Si enunci e si dimostri il teorema della radice razionale.

Esercizio 10.2 (Facoltativo). Mostrate che la matrice, a coefficienti in un campo F,

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ & & & & \ddots & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \dots & -a_{n-2} & -a_{n-1} \end{bmatrix}$$

è radice del polinomio

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n.$$

Esercizio 10.3. Sia F un campo.

(1) Si mostri che F ha caratteristica o 0 o un numero primo p.
(2) Si mostri che
   (a) se F ha caratteristica 0, allora è una estensione di $\mathbf{Q}$;
   (b) se F ha caratteristica un primo p, allora è estensione di $\mathbf{F}_p$.

Esercizio 10.4. Sia A un anello di caratteristica p.

(1) Si mostri che per ogni $a \in A$ si ha $p \cdot a = 0$. (Qui $p \cdot a$ indica il multiplo p-simo di a.)
(2) Sia A commutativo. Si mostri che per $a, b \in A$ si ha
$$(a+b)^p = a^p + b^p.$$
(3) Nel punto precedente, si può dare per buono che in un anello *commutativo* valga la regola del bionomio di Newton. Fate vedere che se A non è commutativo, la regola in generale non vale. (SUGGERIMENTO: Prendete A come l'anello delle matrici 2×2 a coefficienti razionali, prendete
$$a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \qquad b = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$
e mostrate che $(a+b)^2 \neq a^2 + 2ab + b^2$.)

Esercizio 10.5. Sia E un campo finito.

(1) Si mostri che la caratteristica di E è un numero primo p, e dunque E è una estensione di $\mathbf{F}_p$.
(2) Si mostri che la dimensione $|E : \mathbf{F}_p| = n$ è finita.
(3) Si mostri che $|\, E \,| = p^n$.
(4) Si mostri che gli elementi di E sono le radici del polinomio
$$f = x^{p^n} - x \in \mathbf{F}_p[x].$$

(5) Sia L il campo di spezzamento di f su $\mathbf{F}_p$. Si mostri che l'insieme

$$E = \{\, \alpha \in L : f(\alpha) = 0 \,\}$$

delle radici di f in L ha p^n elementi, è un sottoanello di L, ed è un campo.

Esercizio 10.6. Sia $F = \mathbf{F}_2 = \{\, 0, 1 \,\}$.

(1) Si mostri che l'unico polinomio (monico e) irriducibile di grado 2 in $F[x]$ è $g = x^2 + x + 1$.
(2) Si mostri che l'estensione $E = F[\alpha]$ di F, ove α è una radice di g (estensione che esiste per ragioni che abbiamo visto), è un campo con 4 elementi, i cui elementi si scrivono in modo unico come

$$a_0 + a_1\alpha, \tag{1}$$

per $a_0, a_1 \in F$.
(3) Si mostri che α ha periodo 3 in $E^\star$, e dunque

$$E^\star = \langle\, \alpha \,\rangle = \left\{\, \alpha^i : i \in \mathbf{Z} \,\right\}.$$

(4) Si costruisca la tabella del logaritmo discreto per E, nel senso di scrivere ogni potenza α^i, per $0 \le i < 3$, nella forma (1).

Esercizio 10.7. Sia $F = \mathbf{F}_3 = \{\, 0, 1, -1 \,\}$.

(1) Si mostri che ci sono tre polinomi monici e irriducibili di grado 2 in $F[x]$ e che sono

$$g_1 = x^2 - x - 1, g_2 = x^2 + x - 1, g_3 = x^2 + 1.$$

(2) Per ogni $i = 1, 2, 3$, si mostri che l'estensione $F[\xi]$ di F, ove ξ è una radice di g_i, è un campo con 9 elementi, i cui elementi si scrivono in modo unico come

$$a_0 + a_1\xi,$$

per $a_0, a_1 \in F$.
(3) Sia $E = F[\gamma]$, ove γ è una radice di g_3. Si mostri che γ ha ordine 4 in $E^\star$, e dunque $\langle\, \gamma \,\rangle \neq E^\star$.
(4) Sia $E = F[\alpha]$, ove α è una radice di g_1. Si mostri che α ha ordine 8 in $E^\star$, e dunque

$$E^\star = \langle\, \alpha \,\rangle.$$

(5) Sia $E = F[\beta]$, ove β è una radice di g_2. Si mostri che β ha ordine 8 in $E^\star$, e dunque

$$E^\star = \langle\, \beta \,\rangle.$$

(6) Si costruisca la tabella del logaritmo discreto per $F[\alpha]$.
(7) Si costruisca la tabella del logaritmo discreto per $F[\beta]$.
(8) Si trovino i polinomi minimi su F di tutti gli elementi di $F[\alpha]$.
(9) Si trovino i polinomi minimi su F di tutti gli elementi di $F[\beta]$.

Esercizio 10.8.

(1) Si trovino tutti i polinomi irriducibili di grado 3 su $\mathbf{F}_2$. (Sono due.)

(2) Si costruisca un campo E con 8 elementi, usando prima l'uno e poi l'altro dei due polinomi trovati nel punto precedente.
(3) Si calcoli la tabella del logaritmo discreto in E (in entrambi i casi).
(4) Si trovino i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi di E.

Esercizio 10.9.

(1) Si trovino tutti i polinomi irriducibili di grado un divisore di 4 su $\mathbf{F}_2$. (Sono due di grado uno, uno di grado due, e tre di grado quattro.)
(2) Si costruisca un campo E con 16 elementi, usando
   (a) prima il polinomio $x^4 + x + 1$,
   (b) poi il polinomio $x^4 + x^3 + 1$.
(3) Si calcoli la tabella del logaritmo discreto in E, in entrambi i casi.
(4) Si trovino i polinomi minimi su $\mathbf{F}_2$ di tutti gli elementi di E, in entrambi i casi.

(SUGGERIMENTO: A proposito dell'ultimo punto, per trovare le radici in E dei polinomi $s = x^2 + x + 1$ e $t = x^4 + x^3 + x^2 + x + 1$, si può notare che

$$x^3 + 1 = (x + 1)s, \qquad x^5 + 1 = (x + 1)t.$$

Dunque una radice di s è anche radice di $x^3 + 1$, dunque ha periodo 3. Allo stesso modo una radice di t ha periodo 5. Ora abbiamo costruito $E = \mathbf{F}_2[\alpha]$, ove α ha periodo 15. Siccome $1 = \alpha^{15} = (\alpha^3)^5 = (\alpha^5)^3$, avrò che α^3 ha periodo 5, e α^5 ha periodo 3.)