Università degli Studi Roma Tre
Anno Accademico 2009/2010
AL2 - Algebra 2
Esercitazione 6
Lunedì 4 Gennaio 2010
http://www.mat.uniroma3.it/users/pappa/CORSI/AL2_09_10/AL2.htm
domande/osservazioni: dibiagio@mat.uniroma1.it

1. (Dikranjan - Aritmetica e algebra - esercizio 11.33)

   Fattorizzare $f(X) = 4X^9 - 4X$ in prodotto di irriducibili in $\mathbb{Q}[X]$, $\mathbb{Z}[X]$, $\mathbb{Z}_3[X]$.

   Soluzione:

   $4X^9 - 4X = 4X(X^8 - 1) = 4X(X^4 - 1)(X^4 + 1) = 4X(X-1)(X+1)(X^2 + 1)(X^4 + 1)$.

   $4 = 2^2$ in $\mathbb{Z}[X]$, mentre in $\mathbb{Z}_3[X]$ e $\mathbb{Q}[X]$ 4 è invertibile (in particolare $4 = 1$ in $\mathbb{Z}_3[X]$). $X - 1$, $X + 1$ sono polinomi di primo grado, quindi irriducibili in $\mathbb{Q}[X]$ e $\mathbb{Z}_3[X]$. Dato che $X - 1$, $X + 1$ sono polinomi primitivi in $\mathbb{Z}[X]$ ed irriducibili in $\mathbb{Q}[X]$ allora sono irriducibili anche in $\mathbb{Z}[X]$. $X^2 + 1$ è un polinomio privo di radici sia in $\mathbb{Q}[X]$ che in $\mathbb{Z}_3[X]$, quindi, essendo di secondo grado, è irriducibile in entrambi i domini. Inoltre essendo $X^2 + 1$ primitivo in $\mathbb{Z}[X]$ allora è irriducibile anche in $\mathbb{Z}[X]$. $X^4 + 1$ non ha radici né in $\mathbb{Q}[X]$ né in $\mathbb{Z}_3[X]$, quindi al più si può scrivere come prodotto di polinomi di secondo grado. Sia $f(X) = (X^2 + aX + b)(X^2 + cX + d)$. Allora necessariamente $a + c = 0, d + ac + b = 0, ad + bc = 0, bd = 1$. In particolare $a = -c$, quindi $d + b = c^2$ e $c(b - d) = 0$. Se $c = 0$ allora $b = -d$, ma l'equazione $-d^2 = 1$ non ha soluzione né in $\mathbb{Q}$ né in $\mathbb{Z}_3$. Quindi $c \neq 0$, da cui $b = d$, e quindi $b^2 = 1$. Si deve anche avere $2b = c^2$. In $\mathbb{Q}$ non è possibile: $b^2 = 1$ implica $b = \pm 1$ ma ± 2 non è un quadrato in $\mathbb{Q}$. In $\mathbb{Z}_3$ $b = 2$, $c = 1$ verifica $b^2 = 1, 2b = c^2$; inoltre tale scelta è compatibile con le altre equazioni. Quindi $X^4 + 1$ è irriducibile in $\mathbb{Q}[X]$, e anche in $\mathbb{Z}[X]$ dato che è un polinomio primitivo, ma è riducibile in $\mathbb{Z}_3[X]$: $X^4 + 1 = (X^2 + 2X + 2)(X^2 + X + 2)$.

2. (Dikranjan - Aritmetica e Algebra - esercizio 11.38)

   Si considerino in $\mathbb{Z}[X]$ i polinomi $f(X) = X^3 + X + 1$ e $g(X) = X^4 + X^2 + 1$ e gli ideali $I = (2, f(X))$, $J = (2, g(X))$. Dire se I, J sono ideali primi o massimali. Decomporre poi $X^4 + X^2 + 1$ in $\mathbb{Z}_7[X]$ nel prodotto di fattori irriducibili .

   Soluzione:

   $\mathbb{Z}[X]$ è un anello commutativo unitario, quindi per studiare la primalità/massimalità di I è sufficiente studiare l'anello quoziente $\mathbb{Z}[X]/I$: se è un campo allora I è massimale, se è un dominio allora I è primo, altrimenti non è né primo né massimale. Per quanto visto durante l'esercitazione, per il terzo teorema di omomorfismo tra anelli $\mathbb{Z}[X]/I \cong \mathbb{Z}_2[X]/(f(X))$. Dato che $\mathbb{Z}_2$ è un campo, allora $\mathbb{Z}_2[X]$ è un dominio euclideo e in particolare un PID, perciò $\mathbb{Z}_2[X]/(f(X))$ o non è un dominio di integrità oppure è un campo, ed è un campo se e solo se $f(X)$ è irriducibile in $\mathbb{Z}_2[X]$.

Dato che $f(X)$ è un polinomio di terzo grado privo di radici in $\mathbb{Z}_2$ allora $f(X)$ è irriducibile, quindi $\mathbb{Z}_2[X]/(f(X))$ è un campo e allora I è un ideale massimale.

Vale analogo discorso per l'ideale J, solo che in questo caso $g(X) = (X^2 + X + 1)^2$ in $\mathbb{Z}_2[X]$, quindi $g(X)$ è riducibile in $\mathbb{Z}_2[X]$, perciò J non è né massimale né primo.

2 è una radice di $X^4 + X^2 + 1 \in \mathbb{Z}_7[X]$. Con Ruffini possiamo scrivere $f(X) = (X-2)(X^3+2X^2+5X+3)$. -2 è una radice di X^3+2X^2+5X+3, quindi $X^3 + 2X^2 + 5X + 3 = (X + 2)(X^2 + 5)$. $X^2 + 5 = X^2 - 9 = (X-3)(X+3)$. Concludendo: $X^4+X^2+1 = (X-2)(X+2)(X-3)(X+3)$.

3. (Dikranjan - Aritmetica e Algebra - esercizio 11.25) Dimostrare che un ideale principale in $\mathbb{Z}[X]$ non è mai massimale.

   Soluzione:

   Supponiamo per assurdo che esista $f(X) \in \mathbb{Z}[X]$ tale che $(f(X))$ sia massimale. $\deg(f(X)) > 0$ altrimenti $f(X) = p$ con p primo in $\mathbb{Z}$, ma in questo caso (p, X) sarebbe un ideale proprio che contiene (p). Sia q un primo in $\mathbb{Z}$ che non divide il coeff. direttore di $f(X)$. $q \notin (f(X))$, quindi $(q, f(X)) = \mathbb{Z}[X]$. In particolare esistono $h(X), g(X) \in \mathbb{Z}[X]$ tali che $qh(X) + f(X)g(X) = 1$. Passando modulo q si ha $\overline{f}(X)\overline{g}(X) = 1$, ma ciò è assurdo, dato che $\deg(\overline{f}(X)) > 0$.

4. Dire se i seguenti quozienti $R := \frac{D[X]}{(f(X))}$ sono domini di integrità o campi:

   (a) $D = \mathbb{Z}, \mathbb{Q}$, $f(X) = 6 + 30X + 36X^2 + 18X^3 + 51X^4$;

   (b) $D = \mathbb{Q}$, $f(X) = 1 + X + 2X^2 + 3X^3$;

   (c) $D = \mathbb{Z}$, $f(X) = 11 + 21X + 15X^2$;

   (d) $D = \mathbb{Z}$, $f(X) = X^4 + 120X^3 + 730X^2 + 17X + 71$.

   Soluzione:

   (a) $f(X) = 3(2+10X+12X^2+6X^3+17X^4)$ con $2+10X+12X^2+6X^3+17X^4$ irriducibile in $\mathbb{Z}[X]$ per il criterio di Eisenstein e quindi anche in $\mathbb{Q}[X]$, dato che è primitivo in $\mathbb{Z}[X]$. Siccome $f(X)$ non è primo (perché riducibile) in $\mathbb{Z}[X]$ allora R non è un dominio di integrità. Siccome $f(X)$ è irriducibile in $\mathbb{Q}[X]$ allora, essendo $\mathbb{Q}[X]$ un ED, $(f(X))$ è un ideale massimale, quindi R è un campo;

   (b) essendo $\mathbb{Q}$ un campo e $f(X)$ di terzo grado allora $f(X)$ è irriducibile se e solo se non ha radici in $\mathbb{Q}$. Un'eventuale radice $\frac{r}{s}$, con $r, s \in \mathbb{Z}$, $MCD(r, s) = 1$ deve essere tale che $r|1$ e $s|3$. Quindi basta controllare $\pm\frac{1}{3}$. $f(\frac{1}{3}) > 0$, $f(-\frac{1}{3}) = \frac{7}{9} \neq 0$. $f(X)$ è irriducibile, quindi essendo $\mathbb{Q}[X]$ un ED, R è un campo;

   (c) per il criterio di Eisenstein $f(X)$ è irriducibile. Allora, essendo $\mathbb{Z}[X]$ un UFD, $(f(X))$ è un ideale primo, quindi R è un dominio di integrità. Per l'esercizio precedente $(f(X))$ non è massimale, quindi R non è un campo;

(d) dato che $f(X)$ è monico possiamo ridurci modulo ogni primo p. Scegliamo $p = 2$. $\overline{f}(X) = X^4 + X + 1$ è irriducibile in $\mathbb{Z}_2[X]$, dato che $\overline{f}(X)$ non ha radici e $\overline{f}(X) \neq (X^2 + X + 1)^2 = X^4 + X^2 + 1$, dove $X^2 + X + 1$ è l'unico polinomio irriducibile di secondo grado in $\mathbb{Z}_2[X]$. Possiamo quindi concludere che $f(X)$ è irriducibile anche in $\mathbb{Z}[X]$. Come nell'esempio precedente, quindi, R non è un campo ma è un dominio di integrità.

5. Determinare gli ideali primi e massimali dell'anello $\mathbb{R}[X]/(X^4 + 1)$.

   Soluzione:

   Per il teorema di corrispondenza, considerando la proiezione canonica (suriettiva) $\pi : \mathbb{R}[X] \to \mathbb{R}[X]/(X^4 + 1)$, per determinare gli ideali primi/massimali di $\mathbb{R}[X]/(X^4 + 1)$ è sufficiente determinare gli ideali primi/massimali di $\mathbb{R}[X]$ che contengono il nucleo $(X^4 + 1)$. Dato che $\mathbb{R}[X]$ è un ED e quindi in particolare un PID, allora gli ideali primi non nulli sono massimali e gli ideali massimali che contengono $X^4 + 1$ sono tutti e soli gli ideali generati dai fattori irriducibili di $X^4 + 1$. In $\mathbb{R}[X]$ $X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$, con $X^2 - \sqrt{2}X + 1$ e $X^2 + \sqrt{2}X + 1$ irriducibili, poiché con discriminante negativo, e distinti. Quindi se $I = (X^2 - \sqrt{2}X + 1) \subset \mathbb{R}[X]$ e $J = (X^2 + \sqrt{2}X + 1) \subset \mathbb{R}[X]$ allora gli ideali massimali di $\mathbb{R}[X]/(X^4 + 1)$ sono $\pi(I)$ e $\pi(J)$.

6. Si consideri l'anello degli interi di Gauss $\mathbb{Z}[i]$ e l'ideale $I = (3+2i)$. Dire se $(2 + i) + I$ è invertibile in $\mathbb{Z}[i]/I$ ed eventualmente determinarne l'inverso.

   Soluzione:

   La norma di $3 + 2i$ è 13, un numero primo. Quindi $3 + 2i$ è irriducibile in $\mathbb{Z}[i]$; siccome $\mathbb{Z}[i]$ è un ED, e in particolare un PID, allora I è un ideale massimale. Quindi $\mathbb{Z}[i]/I$ è un campo. Siccome $(2 + i) + I \neq I$, cioè $(2 + i) + I$ non è l'elemento nullo di $\mathbb{Z}[i]/I$, allora $(2 + i) + I$ è senz'altro invertibile in $\mathbb{Z}[i]/I$. Troviamone l'inverso, utilizzando l'algoritmo euclideo per il calcolo del MCD tra $3 + 2i$ e $2 + i$ e la relativa identità di Bézout. $3 + 2i = 2(2 + i) - 1$, quindi $1 = 2(2 + i) - (3 + 2i)$, quindi $1 + I = (2(2 + i)) + I - (3 + 2i) + I = (2 + I)((2 + i) + I)$, perciò $2 + I$ è l'inverso di $(2 + i) + I$ in $\mathbb{Z}[i]/I$.

7. Sia $K := \frac{\mathbb{Z}_3[X]}{I}$, con $I := (X^2 + X - 1)$. Dimostrare che K è un campo, determinarne il numero degli elementi e calcolare l'inverso di $X + I$.

   Soluzione:

   $X^2 + X - 1$ è un polinomio di secondo grado privo di radici in $\mathbb{Z}_3$. Quindi è irriducibile. Dato che $\mathbb{Z}_3[X]$ è un ED, allora I è un ideale massimale e K è un campo. K ha 9 elementi, dato che $X^2 + X - 1$ è di secondo grado. Per calcolare l'inverso di $X + I$ utilizziamo l'algoritmo euclideo per il calcolo del MCD, in $\mathbb{Z}_3[X]$, tra X e $X^2 + X - 1$. $X^2 + X - 1 = X(X + 1) - 1$, quindi $1 = -(X^2 + X - 1) + X(X + 1)$. Allora l'inverso di $X + I$ è $(X + 1) + I$.

8. Si consideri il polinomio $f(X) = X^3 + X + 1 \in \mathbb{Q}[X]$ e l'ideale I da esso generato.

(a) Verificare che $f(X)$ è irriducibile in $\mathbb{Q}[X]$.

(b) Si consideri $K := \mathbb{Q}[X]/I$. Dimostrare che K è un campo. Calcolare $[K : \mathbb{Q}]$.

(c) Sia $\theta := X + I \in K$. Esprimere ciascuno dei seguenti elementi nella base $\{1, \theta, \theta^2\}$: θ^4, θ^5, $3\theta^5 - \theta^4+2$, $(\theta^2 + 2\theta + 2)^{-1}$.

Soluzione:

(a) $f(X)$ è un polinomio privo di radici e di terzo grado in $\mathbb{Q}[X]$, dove $\mathbb{Q}$ è un campo. Quindi $f(X)$ è irriducibile.

(b) Siccome $\mathbb{Q}[X]$ è un ED e $f(X)$ è irriducibile allora I è un ideale massimale e di conseguenza K è un campo. Per il teorema di Kronecker $[K : \mathbb{Q}] = 3$.

(c) Per il teorema di Kronecker $K = \{a_0+a_1\theta+a_2\theta^2 | a_0, a_1, a_2 \in \mathbb{Q}\}$, con $\{1, \theta, \theta^2\}$ base di K su $\mathbb{Q}$. In base al teorema di divisione con resto nel dominio euclideo $\mathbb{Q}[X]$ possiamo scrivere: $X^4 = X(X^3+X+1)-(X^2 + X)$, quindi $\theta^4 = -\theta^2 - \theta$, oppure dato che in K $\theta^3 + \theta + 1 = 0$ allora $\theta^3 = -\theta - 1 \Rightarrow \theta^4 = -\theta^2 - \theta$; $X^5 = (X^2 - 1)(X^3 + X + 1) - X^2+X+1$, quindi $\theta^5 = -\theta^2+\theta+1$, oppure $\theta^5 = \theta\theta^4 = \theta(-\theta^2-\theta) = -\theta^3 - \theta^2 = \theta + 1 - \theta^2$. Allora $3\theta^5 - \theta^4 + 2 = -2\theta^2 + 4\theta + 5$. Per calcolare l'inverso di $\theta^2 + 2\theta + 2$ utilizziamo l'algoritmo euclideo per il calcolo del MCD tra $X^3 + X + 1$ e $X^2 + 2X + 2$ in $\mathbb{Q}[X]$: $13/9 = (X^3+X+1)(-X/3-1/9)+(1+(X-2)(X/3+1/9))(X^2+2X+2)$, quindi $13/9 + I = ((X^2 + 2X + 2) + I)((X^2/3 - 5/9X + 7/9) + I)$, quindi $(\theta^2 + 2\theta + 2)^{-1} = 9/39\theta^2 - 5/13\theta + 7/13$.