Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2003/2004
AL2 - algebra 2, gruppi, anelli e campi
Tutorato - Soluzioni
16 dicembre 2003

1. Provare che se D è un dominio d'integrità tale che $D[X]$ è un PID, allora D è un campo.

   (Soluzione suggerita da Livia Corsi)

   Si consideri l'omomorfismo $\phi : D[X] \to D$ t.c. $\phi(f(x)) = f(0)\ \forall f(x) \in D[X]$. ϕ è evidentemente un omomorfismo suriettivo. $\ker\phi$ è un ideale non nullo di $D[X]$ ($X \in \ker\phi$). Per il teorema fondamentale di omom. tra anelli si ha che $D[X]/\ker\phi \simeq D$. Siccome per ipotesi D è un dominio di integrità segue che $\ker\phi$ è un ideale primo di $D[X]$. Ma $D[X]$ per ipotesi è un PID e quindi ogni ideale primo non nullo è anche massimale: perciò $D[X]/\ker\phi$ è un campo e quindi D è un campo.

2. Si consideri nell'anello $\mathbb{Z}_7[X]$ il polinomio $g(X) = X^2 + X + 1$.

   (a) Stabilire se l'ideale $I = (g(X))$ è primo in $\mathbb{Z}_7[X]$.

   (b) Calcolare il numero degli elementi dell'anello quoziente $\mathbb{Z}_7[X]/I$.

   (c) Scrivere nella forma $(a+bX)+I$ l'inverso moltiplicativo dell'elemento invertibile $(X^4 + X^3 + 5X^2 + 3X + 2) + I$.

   (a) $\mathbb{Z}_7[X]$ è un dominio euclideo, quindi in particolare un PID. Perciò I è primo sse $g(X)$ è primo sse $g(X)$ è irriducibile. Siccome $g(X)$ è un polinomio di secondo grado, esso è irriducibile sse non ha radici in $\mathbb{Z}_7$. Si noti che $g(2) = 0$, quindi $g(X)$ è riducibile (in effetti $g(X) = (X + 3)(X + 5)$).

   (b) Consideriamo prima di tutto gli elementi di $\mathbb{Z}_7[X]/I$ scrivibili come $(aX + b) + I$, al variare di $a, b \in \mathbb{Z}_7$. Se $(a, b) \neq (a', b')$ allora $(aX + b) + I \neq (a'X + b') + I$, visto che $(a - a')X + (b - b') \in I \Leftrightarrow a = a'$ e $b = b'$ (infatti I, oltre al pol. nullo contiene solo pol. di grado ≥ 2). Quindi $\mathbb{Z}_7[X]/I$ ha almeno $7 * 7 = 49$ elementi. Inoltre ogni elemento di $\mathbb{Z}_7[X]/I$ è del tipo $f(X) + I$, con $f(X) \in \mathbb{Z}_7[X]$. Poichè però $\mathbb{Z}_7[X]$ è un ED (dominio euclideo), si può effettuare la divisione con resto di $f(X)$ per $X^2 + X + 1$. Sia $r(X)$ tale resto. O $r(X) = 0$ oppure $deg(r(X)) < 2$; inoltre chiaramente $r(X) + I = f(X) + I$. Quindi l'anello considerato ha esattamente 49 elementi.

   Il risulato precedente si può generalizzare: se K è un campo finito con n elementi e se si prende nell'anello $K[X]$ un ideale J (forzatamente principale) generato da $h(X)$ di grado m, allora la cardinalità dell'anello $K[X]/J$ è n^m.

   (c) Sia $f(x) = X^4 + X^3 + 5X^2 + 3X + 2$. Procederemo in due modi:

   Siccome $\mathbb{Z}_7[X]$ è un ED, attraverso l'algoritmo delle divisioni successive è possibile trovare un massimo comun divisore tra $f(X)$ e $g(X)$ ed esprimerlo attraverso un'identità di Bezout:

$f(X) = g(X)(X^2 + 4) + (6X + 5)$
$g(X) = (6X + 5)(6X + 1) + 3$
e quindi $3 = g(X)[1 - (6X + 1)(X^2 + 4)] + f(X)(X + 6)$
Moltiplicando ora entrambi i membri dell'ultima uguaglianza per l'inverso moltiplicativo di 3 (cioè 5), otteniamo
$1 = g(X)5[1 - (6X + 1)(X^2 + 4)] + f(X)(5X + 2)$.
Allora $(5X+2)+I$ è l'inverso di $f(x)+I$ in $\mathbb{Z}_7[X]/I$. Questo perché, per costruzione, $f(X)(5X + 2) - 1 \in (g(X)) = I$.

Poniamo $t = X + I$. Dato che $I = (g(X))$, $g(t) = 0$ in $\mathbb{Z}_7[X]/I$, cioè $t^2 + t + 1 = 0$. $f(X) + I = f(X + I) = f(t) = 6t + 5$. Cerchiamo per $6t+5$ un inverso della forma $at+b$ $(a, b \in \mathbb{Z}_7)$. $(6t+5)(at+b) = (6at^2+ (6b+5a)t+5b) = 6a(-t-1)+(6b+5a)t+5b = (6b-a)t+(5b-6a)$
Perciò $(6t + 5)(at + b) = 1$ sse $6b = a$ e $5b - 6a = 1$, cioè $b = 2, a = 5$
L'inverso di $f(X) + I$ è quindi $(5X + 2) + I$.

3. Nell'anello $\mathbb{Z}_3[X]$ si considerino i seguenti polinomi:

$$f(X) = X^3 + 2X^2 + X + 2 \qquad g(X) = X^4 + 2X^2 + 1.$$

(a) Stabilire se gli ideali $I = (f(X))$ e $J = (g(X))$ sono primi in $\mathbb{Z}_3[X]$.
(b) Provare che esiste un unico ideale massimale M che contiene sia I che J.
(c) Descrivere il campo $\mathbb{Z}_3[X]/M$.

(a) I e J sono ideali primi sse $f(X)$ e $g(X)$ sono polinomi irriducibili (cfr. ex. 2a). $f(X)$ è un polinomio di terzo grado, quindi è irriducibile sse non ha radici in $\mathbb{Z}_3$. $f(1) = 0$, perciò $f(X)$ è riducibile. Si trova che la fattorizzazione di $f(X)$ in irriducibili è $f(X) = (X + 2)(X^2 + 1)$. $g(X) = (X^2 + 1)^2$, quindi anche $g(X)$ è riducibile.
(b) Ogni ideale massimale che contiene sia I che J deve contenere $I + J$. Siccome $\mathbb{Z}_3[X]$ è un PID $I + J = (MCD(f(X), g(X)) = (X^2 + 1)$. Ma $X^2 + 1$ è irriducibile, quindi $I + J$ è massimale. Perciò $\exists!$ ideale massimale M che contiene $I + J$: $I + J$ stesso.
(c) Il campo $\mathbb{Z}_3[X]/M$ è un campo finito con $3^2 = 9$ elementi (cfr. ex. 2b)

4. Si consideri il polinomio

$$f(X) = 3X^2 + 4X + 3 \in \mathbb{Z}_m[X].$$

(a) Stabilire se, per $m = 2, 3, 7$, $f(X)$ è irriducibile.
(b) Per $m = 5$, spiegare perchè le fattorizzazioni $(3X + 2)(X + 4)$ e $(4X + 1)(2X + 3)$ di $f(X)$ in $\mathbb{Z}_5[X]$ non contraddicono la fattorialità dell'anello $\mathbb{Z}_5[X]$.
(c) Determinare gli elementi idempotenti di $\mathbb{Z}_5[X]/I$, dove I è l'ideale generato da $f(X)$ in $\mathbb{Z}_5[X]$.

(a) Per $m = 2$ $f(X) = X^2 + 1 = (X+1)^2 \Rightarrow f(X)$ è riducibile.
Per $m = 3$ $f(X) = X \Rightarrow f(X)$ è irriducibile.
Per $m = 7$ $f(X) = 3X^2 + 4X + 3 = (X+2)(X+4) \Rightarrow f(X)$ è riducibile.

(b) Perché $(4X+1) = -(X+4)$ e $(2X+3) = -(3X+2)$, cioè i fattori delle due fattorizzazioni sono associati (e ricordiamo che l'unicità della fattorizzazione si ha a meno di associati)

(c) Sia g(X)=X+4, elemento irriducibile di $\mathbb{Z}_3[X]$ e sia $A = \mathbb{Z}_3[X]/I$. Si noti, prima di tutto, che $3(X+4) = 3X+2$, quindi $I = (f(X)) = ((X+4)^2) = (g(X)^2)$. Sia $a \in A$ elemento idempotente, cioè $a^2 - a = 0$. Siccome $a \in A$, $\exists\, h(X) \in \mathbb{Z}_3[X]$ t.c. $a = f(X) + I$. Da $a^2 - a = 0$ segue che $f(X)^2 - f(X) \in I$, ovvero $g(X)^2 | f(X)(f(X)-1)$. Dato che $\mathbb{Z}_3[X]$ è in particolare un UFD e visto che $MCD(f(X), f(X)-1) = 1$ si ha che $g(X)^2 | f(X)$ oppure $g(X)^2 | f(X) - 1$, cioè $a = 0$ oppure $a = 1$. Questi sono gli unici elementi idempotenti.

5. Si consideri nell'anello $\mathbb{Z}_5[X]$ il polinomio $f(X) = X^4 + 2$; sia $I = (X^4 + 2)$.

   (a) Verificare che il polinomio $f(X)$ è irriducibile in $\mathbb{Z}_5[X]$.

   (b) Descrivere il campo $K = \mathbb{Z}_5[X]/I$.

   (c) Trovare in K l'inverso dell'elemento $(X^2 + X + 1) + I$.

   (a) Siccome il polinomio ha grado superiore a tre, non è sufficiente verificare che non ha radici in $\mathbb{Z}_5$ per concludere la sua irriducibilità. Il fatto che non abbia radici mostra solamente che $f(X)$ non si può ridurre con un pol. di primo grado e uno di terzo. Si deve quindi anche escludere che si possa scrivere come prodotto di due polinomi di secondo grado. Lo si può mostrare per assurdo.

   (b) il campo K è un campo finito con $5^4 = 625$ elementi (cfr. ex. 2b).

   (c) L'inverso è $(2X^3 + X^2 + 2X + 2) + I$ (cfr. ex. 2c).

6. Sia p un numero primo dispari.

   (a) Provare che per $a \in \mathbb{Z}_p^\star$ l'equazione $X^2 = a$ ha una soluzione se e solo se $a^{\frac{p-1}{2}} = 1$.
   (Sugg. : $\mathbb{Z}_p^\star$ è un gruppo ciclico.)

   (b) Usando il punto precedente, stabilire se il polinomio $X^2 - 6$ è irriducibile in $\mathbb{Z}_{17}[X]$.

   (c) Sia $I = (X^2 - 6)$. Cosa si può dire dell'anello quoziente $A = \frac{\mathbb{Z}_{17}}{I}$?

   (d) Determinare in A l'inverso dell'elemento $2t - 1$ con $t = X + I$.

   (a) Se $X^2 = a$ ha una soluzione allora $\exists\, b \in Z_p^\star$ t.c. $b^2 = a$. Perciò $a^{\frac{p-1}{2}} = b^{p-1} = 0$ per il piccolo teorema di Fermat (o semplicemente perchè la cardinalità di $Z_p^\star$ è $p-1$).

Sia g un generatore di $Z_p^\star$. Allora $\exists\ h \in \mathbb{Z}$ t.c. $g^h = a$. Se $a^{\frac{p-1}{2}} = 1$ allora $g^{h\frac{p-1}{2}} = 1$. Essendo g un generatore si deve avere che Card$(Z_p^\star)$ $= p-1|h\frac{p-1}{2}$ e questo implica che $2|h$. Ma allora $g^{\frac{h}{2}}$ è soluzione di $X^2 - a$.

(b) In $\mathbb{Z}_{17}$ $6^8 = 2^4 = -1$. Quindi $X^2 - 6$ non ha radici in $\mathbb{Z}_{17}[X]$ e perciò è irriducibile.

(c) I è un ideale generato da un elemento irriducibile in un PID, quindi è massimale. Ma allora A è un campo con $17^2 = 289$ elementi (cfr. ex. 2b)

(d) L'inverso è $6t + 3$ (cfr. ex. 2c).