Università degli Studi Roma Tre
Anno Accademico 2006/2007
AL2 - Algebra 2
Esercitazione 6
Martedì 19 Dicembre 2006

1. (Appello A, a.a. 2003/2004). Siano X un insieme non vuoto e $\mathcal{P}(X)$ l'insieme delle sue parti.

   Allora $(\mathcal{P}(X), +, \cdot)$, dove $+$ è la differenza simmetrica, $A + B = A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$ con A, B sottoinsiemi di X, e $\cdot$ è la intersezione, è un anello commutativo unitario; inoltre tale anello è booleano, cioé per ogni $A \in \mathcal{P}(X)$ si ha che $A^2 = A$.

   (a) Provare che $\mathcal{P}(X)$ è un dominio di integrità se, e solo se, $|X| = 1$.

   (b) Sia $x \in X$; sia
   $$I_x := \{A \in \mathcal{P}(X) \mid x \notin A\}.$$
   Provare che I_x è un ideale massimale di $\mathcal{P}(X)$.

   (c) Provare che $\mathcal{P}(X)/I_x \cong \mathbb{Z}_2$.

   (d) Se $|X| = 3$, determinare tutti gli ideali di $\mathcal{P}(X)$ e mostrare che ogni ideale massimale è del tipo I_x per qualche $x \in X$.

   Prima di tutto è opportuno notare che l'unità 1 di $\mathcal{P}(X)$ è $X \in \mathcal{P}(X)$ e che l'elemento neutro additivo 0 è l'insieme vuoto $\emptyset \in \mathcal{P}(X)$. Per ogni $A \in \mathcal{P}(X)$, $A + A = 0$. Inoltre, per ogni $A \in \mathcal{P}(X)$ indicheremo con A^c il complementare di A in X (i.e. $A^c = X \setminus A$).

   (a) Se $|X| = 1$ allora $\mathcal{P}(X) = \{\emptyset, X\}$ che è evidentemente un dominio di integrità (isomorfo al campo $\mathbb{Z}_2$). Viceversa: sia $A \in \mathcal{P}(X)$. Allora $A \cdot A^c = \emptyset = 0$. Essendo per ipotesi $\mathcal{P}(X)$ un dominio di integrità segue che A o A^c è l'insieme vuoto, quindi ogni $A \in \mathcal{P}(X)$ è o l'insieme vuoto o X stesso, quindi $|\mathcal{P}(X)| = 2$ da cui $|X| = 1$.

   (b) I_x è un ideale, infatti: se $A, B \in I_x$ allora, per definizione, $x \notin A, x \notin B$, cioé $x \notin A \cup B$, quindi $x \notin A - B = A + B = (A \cup B) \setminus (A \cap B)$; se $A \in I_x$ e $B \in \mathcal{P}(X)$ qualsiasi, allora $x \notin A \cdot B = A \cap B$, quindi $A \cdot B \in I_x$. Dimostriamo ora che I_x è massimale. Sia $J_x \supsetneq I_x$ ideale di $\mathcal{P}(X)$. Dobbiamo dimostrare che $J_x = \mathcal{P}(X)$, cioè che $1 = X \in J_x$. Dato che J_x contiene strettamente I_x, allora $\exists A \in J_x$ t.c. $x \in A$. Ma allora $A^c \in I_x$ per definizione, da cui $A^c \in J_x$ per ipotesi. Perciò sia A sia A^c sono in J_x, perciò anche $A + A^c \in J_x$, cioè $(A \cup A^c) \setminus (A \cap A^c) = X \setminus \emptyset = X \in J_x \Rightarrow J_x = \mathcal{P}(X)$.

   (c) Consideriamo l'applicazione $\phi_x : \mathcal{P}(X) \to \mathbb{Z}_2$ definita così: $\phi_x(A) = 1$ se $x \in A$, $\phi_x(A) = 0$ se $x \notin A$. ϕ è un omomorfismo unitario: $\phi(X) = 1$, $\phi_x(A + B) = \phi_x(A) + \phi_x(B)$, $\phi_x(A \cdot B) = \phi_x(A)\phi_x(B)$ per ogni $A, B \in \mathcal{P}(X)$. ϕ_x è un omomorfismo suriettivo ($\phi_x(\emptyset) = 0$, $\phi_x(X) = 1$). Il nucleo di ϕ_x è, per definizione, I_x. Per il teorema fondamentale di omomorfismo di anelli, allora, $\mathcal{P}(X)/I_x \cong \mathbb{Z}_2$. Si

noti che abbiamo anche nuovamente dimostrato che I_x è un ideale (nucleo di ϕ_x), e che è un ideale massimale ($\mathbb{Z}_2$ è un campo).

(d) Daremo due diverse risoluzioni per questo punto, la prima più concreta ed intuitiva, la seconda più generale e teorica.

1° metodo. Sia $X := \{1, 2, 3\}$. Prima di tutto tra gli ideali di $\mathcal{P}(X)$ vi sono i due ideali banali $\mathcal{P}(X)$ e $\{\emptyset\}$. Dato che $|X| = 3$ allora $|\mathcal{P}(X)| = 8$, quindi gli ideali non banali di $\mathcal{P}(X)$, dovendo anzitutto essere sottogruppi di $\mathcal{P}(X)$, hanno o 2 o 4 elementi. Non solo: (*) se J è un ideale e $A \in J$ allora, per definizione di ideale, $\mathcal{P}(A) \subseteq J$ (infatti: sia $B \in \mathcal{P}(A)$. Allora $B \subseteq A \Rightarrow B \cdot A = B \Rightarrow B \in J$).

I sottogruppi con due elementi sono tutti e soli gli insiemi $\{\emptyset, A\}$, con $A \in \mathcal{P}(X), A \neq \emptyset, X$ (per il 'tutti' basta osservare che ogni elemento di $\mathcal{P}(X)$ ha ordine 2). Allora gli ideali con due elementi sono tutti e soli gli insiemi $\{\emptyset, B\}$ con B singleton ('soli' per (*) e 'tutti' perché l'intersezione tra un singleton e un qualsiasi altro insieme è o il singleton o l'insieme vuoto). Quindi gli ideali con due elementi sono $\{\emptyset, \{1\}\}, \{\emptyset, \{2\}\}, \{\emptyset, \{3\}\}$.

Cerchiamo ora gli ideali con quattro elementi. Gli insiemi I_1, I_2, I_3 (definiti come in (b)) sono ideali e hanno quattro elementi (I_1, ad esempio, è $\{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$). Un qualsiasi ideale J con quattro elementi è del tipo $\{\emptyset, A, B, C\}$ con $A, B, C \in \mathbb{P}(X)$, A, B, C distinti e diversi da X e dall'insieme vuoto. Non potendo sia A che B che C avere contemporaneamente cardinalità 1 (se $|A| = 1, |B| = 1$ allora $A \neq B \Rightarrow |A + B| = 2$) allora almeno uno tra A, B, C ha cardinalità 2. Supponiamo quindi $|C| = 2$, cioé C è il complementare di un singleton $\{@\}$ ($@ \in X$). Ma allora per (*) $\{\emptyset, A, B, C\} = \mathcal{P}(C)$ cioé $J = I_@$. Siccome ogni ideale con due elementi è contenuto in almeno un certo $I_@$ e ogni $I_@$ è un ideale massimale, anche l'ultima tesi è dimostrata.

2° metodo. Siano $R_1, \ldots, R_n$ anelli commutativi unitari. Sia $R := R_1 \times \ldots \times R_n$. Sia $\pi_i : R \to R_i$ l'omomorfismo proiezione sull'i-esimo fattore. Per ogni i definiamo $\delta_i := (0, \ldots, 0, \underbrace{1}_{\text{posto i-esimo}}, 0, \ldots, 0) \in R$.

E' chiaro che se $Y_1 \subseteq R_1, \ldots, Y_n \subseteq R_n$ sono ideali, allora $Y_1 \times \ldots \times Y_n$ è un ideale di $R = R_1 \times \ldots \times R_n$. Mostriamo ora che vale anche il viceversa: sia J ideale di R. Per ogni i, $1 \leq i \leq n$, definiamo $J_i := \pi_i(J)$. Per la suriettività di π_i si ha che J_i è un ideale. E' anche chiaro che $J \subseteq J_1 \times \ldots \times J_n$. Sia ora $(j_1, \ldots j_n) \in J_1 \times \ldots \times J_n$. Per definizione di J_i esistono elementi $s_1, \ldots, s_n \in J$ t.c. $\pi_i(s_i) = j_i$. Ma allora $(j_1, \ldots, j_n) = \sum_{i=1}^{n} s_i \cdot \delta_i$ appartiene a J (per def. di ideale), e quindi $J = J_1 \times \ldots \times J_n$.

Osserviamo, inoltre, che nel caso in cui, per ogni i, $R_i = K$ campo

fissato, allora tutti e soli gli ideali di $\underbrace{K \times \ldots \times K}_{\text{n volte}}$ sono del tipo

$$\mathcal{Y}_{l_1,\ldots,l_t} := K\times\ldots\times K\times \underbrace{\{0\}}_{\text{posto } l_1-\text{esimo}} \times K\times\ldots\times K\times \underbrace{\{0\}}_{\text{posto } l_t-\text{esimo}} \times\ldots\times K$$

per ogni $1 \leq l_1 < \ldots < l_t \leq n$, $1 \leq t \leq n$. Non solo: è anche chiaro che $\mathcal{Y}_{l_1,\ldots,l_t} = \mathcal{Y}_{l_1} \cap \ldots \cap \mathcal{Y}_{l_t}$.

Sia X insieme finito di cardinalità n, $X = \{1, \ldots, n\}$. Sia $R := \underbrace{\mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{\text{n volte}}$. Consideriamo l'omomorfismo di anelli $\phi : \mathcal{P}(X) \to R$, definito come $\phi = (\phi_1, \ldots, \phi_n)$ (cfr. punto (c)). Per quanto visto al punto (c) ϕ è effettivamente un omomorfismo. Inoltre ϕ è suriettivo: l'n-pla di R che presenta gli 1 nei posti $l_1, \ldots, l_n$ è immagine, tramite ϕ, dell'insieme $\{l_1, \ldots, l_n\} \in \mathcal{P}(X)$. ϕ è anche iniettivo: solo $\emptyset$ ha immagine nulla. Quindi ϕ è un isomorfismo. Ma allora tutti e soli gli ideali di $\mathcal{P}(X)$ sono $\phi^{-1}(\mathcal{Y}_{l_1} \cap \ldots \cap \mathcal{Y}_{l_t}) = \phi^{-1}(\mathcal{Y}_{l_1}) \cap \ldots \cap \phi^{-1}(\cap \mathcal{Y}_{l_t})$. Ora, se $1 \leq v \leq n$, è facile convincersi che $\phi^{-1}(\mathcal{Y}_v) = I_v$ della def. al punto (b). Quindi tutti e soli gli ideali di $\mathcal{P}(X)$ sono tutte e sole le possibili intersezioni tra gli ideali massimali I_x, con $x \in X$. E' anche chiaro, quindi, che gli I_x, $x \in X$, sono tutti e soli gli ideali massimali di $\mathcal{P}(X)$.

Nel caso specifico, se $X = \{1, 2, 3\}$, gli ideali di $\mathcal{P}(X)$ sono $\emptyset$, X, I_1, I_2, I_3, $I_1 \cap I_2$, $I_1 \cap I_3$, $I_2 \cap I_3$.

2. (Appello B, a.a. 2003/2004). Sia $C([0,1])$ l'anello delle funzioni continue reali definite sull'intervallo $[0,1]$. Sia $T \subseteq [0,1]$; si ponga

$$I(T) := \{f \in C([0,1]) \ t.c. \ f(y) = 0 \ \forall y \in T\}.$$

   (a) Provare che $C([0,1])$ non è un dominio di integrità.

   (b) Caratterizzare gli elementi invertibili di $C([0,1])$.

   (c) Provare che $I(T)$ è un ideale di $C([0,1])$

   (d) Se $x \in [0,1]$, si ponga $M_x := I(\{x\})$.

      i. Provare che M_x è un ideale massimale di $C([0,1])$.

      ii. Determinare, a meno di isomorfismo, $C([0,1])/M_x$.

   (a) Basta trovare due funzioni, f e g, continue su $[0,1]$, non nulle, il cui prodotto è la funzione nulla. Ad esempio:

$$f(x) = \begin{cases} 0 & x \leq \frac{1}{2} \\ x - \frac{1}{2} & x > \frac{1}{2} \end{cases}$$

$$g(x) = \begin{cases} x - \frac{1}{2} & x \leq \frac{1}{2} \\ 0 & x > \frac{1}{2} \end{cases}$$

   f e g sono continue per il lemma dell'incollamento, non sono la funzione nulla ma il loro prodotto è 0.

(b) Sia $f \in C([0,1])$ invertibile. Allora $\exists g \in C([0,1])$ t.c. $fg = 1$, cioé $\forall x \in [0,1]\ f(x)g(x) = 1 \Rightarrow f(x) \neq 0$. Viceversa: sia $f \in C([0,1])$, f mai nulla. Allora è definita la funzione $g(x) = 1/f(x)$, anch'essa continua. Perciò $f \in C([0,1])$ è invertibile se, e solo se, non si annulla mai.

(c) $\forall x \in T, \forall f, g \in I(T), \forall k \in C([0,1])$, si ha $(f-g)(x) = f(x) - g(x) = 0 - 0 = 0 \Rightarrow (f-g) \in I(T)$, $(kf)(x) = k(x)f(x) = 0 \Rightarrow kf \in I(T)$. Quindi $I(T)$ è un ideale.

(d) Se $x \in [0,1]$, si ponga $M_x := I(\{x\})$.

i. Sia $J_x \supsetneq M_x$ ideale di $C([0,1])$. Allora $\exists f \in J$ t.c. $f(x) = a, a \in \mathbb{R}^*$. Si riguardi a come funzione costante su $[0,1]$. $a \in C([0,1])$. Allora $f - a \in M_x$, e perciò $f - a \in J_x$. Ma allora anche $a = f - (f - a) \in J_x \Rightarrow 1 \in J_x \Rightarrow J_x = C([0,1])$. Quindi M_x è massimale.

ii. Sia $\phi_x : C([0,1]) \to \mathbb{R}$ così definita: $\forall f \in C([0,1]), \phi_x(f) := f(x)$. f è un omomorfismo suriettivo e unitario di anelli. Per definizione il nucleo è proprio M_x. Per il teorema di omomorfismo di anelli, quindi, $C([0,1])/M_x \cong \mathbb{R}$. Si osservi che, in questo modo, si è nuovamente dimostrato che M_x è un ideale (in quanto nucleo di un omomorfismo) e che è massimale (in quanto $\mathbb{R}$ è un campo).

3. (Appello A, a.a. 2003/2004). Sia $r \in \mathbb{Z}_p$, con p numero primo. Sia

$$A := \left\{ \begin{pmatrix} a & b \\ br & a \end{pmatrix}, a, b \in \mathbb{Z}_p \right\}.$$

(a) Verificare che A è un sottoanello commutativo ed unitario dell'anello $M_2(\mathbb{Z}_p)$ con p^2 elementi.

(b) Provare che A è un sottocampo di $M_2(\mathbb{Z}_p)$ se e solo se r non è un quadrato in $\mathbb{Z}_p$.

(c) Determinare per quali $r \in \mathbb{Z}_{11}$ l'anello A è un campo.

(d) Determinare un isomorfismo esplicito tra A e $\mathbb{Z}_p[X](X^2 - r)$.

(a) Si verifica facilmente che A è un sottogruppo. Inoltre la matrice identità $\mathbb{I}$ appartiene a A. Inoltre, per ogni $a, b, a', b' \in \mathbb{Z}_p$

$$\begin{pmatrix} a & b \\ br & a \end{pmatrix} \begin{pmatrix} a' & b' \\ b'r & a' \end{pmatrix} = \begin{pmatrix} aa' + bb'r & ab' + a'b \\ (a'b + ab')r & aa' + bb'r \end{pmatrix} = \begin{pmatrix} a' & b' \\ b'r & a' \end{pmatrix} \begin{pmatrix} a & b \\ br & a \end{pmatrix}.$$

Perciò A è un sottoanello commutativo di $M_2(\mathbb{Z}_p)$.

(b) Sia

$$m = \begin{pmatrix} a & b \\ br & a \end{pmatrix}$$

la generica matrice in A $(a, b \in \mathbb{Z}_p)$.
$\exists m^{-1} \in A \Leftrightarrow \det(m) = a^2 - b^2 r \neq 0$ (se $\det(m) \neq 0$ la matrice m^{-1} esiste in $M_2(\mathbb{Z}_p)$ e sta ancora in A).

Se r è un quadrato in $\mathbb{Z}_p$ allora $\exists x \in \mathbb{Z}_p$ t.c. $r = x^2$. Ma allora poniamo $b = 1$ e $a = x$. In questo caso $\det(m) = 0$ quindi m, pur non essendo l'elemento nullo, non è invertibile. Perciò A non è un campo.

Viceversa: supponiamo che A non è un campo. Questo vuol dire che esiste almeno un elemento di A non nullo e non invertibile. Sia m tale elemento. Ma allora $det(m) = 0$, cioé $a^2 - b^2 r = 0$. Chiaramente $b \neq 0$ altrimenti $a = 0$ e m sarebbe la matrice nulla. Quindi b è invertibile in $\mathbb{Z}_p$, quindi $r = a^2(b^{-1})^2$, cioé r è un quadrato in $\mathbb{Z}_p$.

(c) In $\mathbb{Z}_{11}$, $0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9, (\pm 4)^2 = 5, (\pm 5)^2 = 3$, quindi, in virtù del punto precedente, A è un campo se, e solo se, $r = 2, 6, 7, 8, 10$.

(d) Sia $I := (X^2 - r)$. Ogni elemento f di $\mathbb{Z}_p[X]/I$ si può scrivere in uno e un solo modo come $(y_f + z_f X) + I$ con $y_f, z_f \in \mathbb{Z}_p$. Sia $\phi : \mathbb{Z}_p[X]/I \to A$ così definito: $\forall f \in \mathbb{Z}_p[X]/I$, $\phi(f) = \begin{pmatrix} y_f & z_f \\ z_f r & y_f \end{pmatrix}$.

Si verifica facilmente che ϕ è un omomorfismo di gruppi, e che ϕ è unitario. ϕ è anche un omomorfismo di anelli, dato che $\forall f, g \in \mathbb{Z}_p[X]/I$, $f = (y_f + z_f X) + I$, $g = (y_g + z_g X) + I$, si ha $fg = (y_f y_g + (y_f z_g + z_f y_g)X + z_f z_g X^2) + I = (y_f y_g + z_f z_g r + (y_f z_g + z_f y_g)X) + I$. ϕ è chiaramente iniettivo e suriettivo, perciò ϕ è l'isomorfismo cercato.

4. (Appello B, a.a. 2003/2004). Sia p un numero primo. Siano

$$R_1 = \mathbb{Z}_p[X]/(X^2 - 2) \text{ ed } R_2 = \mathbb{Z}_p[X]/(X^2 - 3).$$

Stabilire se $R_1 \cong R_2$ per $p = 2, 3, 11$.

Sia $p = 2$. Si consideri l'omomorfismo $\mathbb{Z}_2[X] \to \mathbb{Z}_2[X]$ definito come $\phi(f(X)) = f(X + 1)$, per ogni $f(X) \in \mathbb{Z}_p[X]$. Allora $\phi((X^2)) = ((X + 1)^2) = (X^2 + 1)$. Quindi $R_1 \cong R_2$.

Sia $p = 3$. $X^2 + 1$ è irriducibile in $\mathbb{Z}_3[X]$ (è di grado 2 e non ha radici). X^2 invece è chiaramente riducibile. Quindi R_1 è un campo, mentre R_2 non è neppure un dominio di integrità. Perciò $R_1 \ncong R_2$.

Sia $p = 11$. $X^2 + 9$ è è irriducibile in $\mathbb{Z}_{11}[X]$ (è di grado 2 e non ha radici). $X^2 + 8$, invece, è riducibile ($5^2 + 8 = 33 \equiv_{11} 0$). Quindi $R_1 \ncong R_2$.

5. Sia $f(X) = X^5 + X^3 + 1 \in \mathbb{Z}_2[X]$. Sia $I = (f(X))$ l'ideale generato da $f(X)$ in $\mathbb{Z}_2[X]$.

(a) Provare che $F := \mathbb{Z}_2[X]/I$ è un campo.

(b) Determinare esplicitamente l'inverso in F dell'elemento $(X^8 + X + 1) + I$.

(c) Determinare un generatore del gruppo moltiplicativo $(F^*, \cdot)$.

(d) Quanti generatori ci sono nel gruppo $(F^*, \cdot)$?

(a) $\mathbb{Z}_2[X]$ è un ED e quindi un PID: per dimostrare che F è un campo basta quindi far vedere che $X^5 + X^3 + 1$ è irriducibile in $\mathbb{Z}_2[X]$ (in un PID, a irriducibile $\Leftrightarrow$ (a) massimale). $X^5 + X^3 + 1$ non ha radici in $\mathbb{Z}_2$, quindi, se fosse riducibile, si dovrebbe poter scrivere come prodotto di un polinomio di grado 3 senza radici ed un polinomio di grado 2 senza radici. L'unico polinomio di grado 2 in $\mathbb{Z}_2[X]$ e senza radici è $X^2 + X + 1$. I polinomi di grado 3 in $\mathbb{Z}_2[X]$ e senza radici sono $X^3 + X + 1$ e $X^3 + X^2 + 1$. Ma $(X^2 + X + 1)(X^3 + X + 1) = X^5 + X^4 + 1 \neq f$ e $(X^2 + X + 1)(X^3 + X^2 + 1) = X^5 + X + 1 \neq f$.

(b) Usiamo l'algoritmo euclideo per la determinazione del MCD e la relativa identità di Bézout: $X^8+X+1 = (X^3+X)f+X^4+X^3+1$, perciò $(X^8+X+1)+I = (X^4+X^3+1)+I$. $f = (X+1)(X^4+X^3+1)+X$, $X^4+X^3+1 = (X^3+X^2)(X)+1$, da cui $1 = (X^4+X^3+1)+(X^3+X^2)(X) = (X^4+X^3+1)+(f+(X+1)(X^4+X^3+1))(X^3+X^2) = f(X^3+X^2)+(X^4+X^3+1)(1+(X+1)(X^3+X^2))$. Quindi $(1+(X+1)(X^3+X^2))+I = (X^4+X^2+1)+I$ è l'inverso di $(X^4+X^3+1)+I$ in F.

(c) F ha $2^5 = 32$ elementi. Quindi F^* è un gruppo con 31 elementi. 31 è un numero primo, quindi ogni elemento di F^*, eccetto l'elemento identità $1 + I$, ha ordine 31 (i.e.: è un generatore): ad esempio possiamo scegliere come generatore $X + I$.

(d) Per quanto detto prima i generatori sono 30 ($30 = \phi(31)$, dove ϕ è la funzione di Eulero).

6. (a) Stabilire quali dei seguenti ideali sono primi e quali massimali:
   i. Per ogni $q \in \mathbb{Q}$ l'ideale di $\mathbb{Q}[X, Y]$ generato da $X - q$.
   ii. l'ideale generato in $\mathbb{Z}[i]$ da $-1 + 3i$ e da 2.
   iii. l'ideale generato in $\mathbb{Q}[X]$ dal polinomio $X^4 + 2X + 2$.
   iv. l'ideale generato in $\mathbb{Z}_{14}$ da $[7]_{14}$.

   (b) Per ciascuno degli ideali non massimali del punto (a) trovare un ideale massimale che lo contenga.

(a) Stabilire quali dei seguenti ideali sono primi e quali massimali:

i. $\forall q \in \mathbb{Q}$, $X - q$ è un polinomio irriducibile. $\mathbb{Q}[X, Y]$ è un UFD, quindi $\forall q \in \mathbb{Q}$, $(X - q)$ è un ideale primo. In nessun caso è un ideale massimale: $(X - q) \subsetneq (X - q, Y)$.

ii. Determiniamo un MCD tra $-1 + 3i$ e 2 usando l'algoritmo euclideo delle divisioni successive: $-1 + 3i = 2i + (-1 + i)$, $2 = (-1+i)(-1-i)$. Perciò un MCD tra $-1+3i$ e 2 è $-1+i$. Quindi $(-1+3i, 2) = (-1+i)$. $-1+i$ ha norma 2, quindi, in particolare, è un elemento irriducibile. $\mathbb{Z}[i]$ è un ED, quindi $(-1 + i)$ è un ideale primo e massimale.

iii. Per il criterio di Eisenstein $X^4 + 2X + 2$ è irriducibile in $\mathbb{Q}[X]$. Quindi, essendo $\mathbb{Q}[X]$ un ED, $(X^4 + 2X + 2)$ è un ideale primo e massimale.

iv. $\mathbb{Z}_{14}/([7]_{14}) \cong \mathbb{Z}_7$, quindi, essendo $\mathbb{Z}_7$ un campo, $([7]_{14})$ è un ideale primo e massimale.

(b) Basta osservare che $(X - q, Y)$ è un ideale massimale. Infatti sia $\phi : \mathbb{Q}[X, Y] \to \mathbb{Q}$ definito come $\phi(f(X, Y)) = f(q, 0)$. ϕ è un omomorfismo unitario di anelli, suriettivo e con nucleo $(X - q, Y)$. Per il teorema fond. di omomorfismo, quindi, $\mathbb{Q}[X, Y]/(X - q, Y) \cong \mathbb{Q}$, quindi $(X - q, Y)$ è un ideale massimale.