Università degli Studi Roma Tre
Anno Accademico 2009/2010
AL2 - Algebra 2
Esercitazione 5
Venerdì 9 Dicembre 2009
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 9.24)

   Sia A un anello commutativo unitario. Dimostrare che $N(A)$ coincide con l'intersezione di tutti gli ideali primi di A.

   Soluzione:

   Sia $x \in N(A)$. Allora esiste n tale che $x^n = 0$. Per ogni P ideale primo di A si ha $0 \in P$, allora $x^n \in P$ e, per definizione di ideale primo, $x \in P$. Quindi per ogni P ideale primo di A, $N(A) \subseteq P$, da cui $N(A) \subseteq \cap_{P \text{ ideale primo}} P$.

   Dimostriamo il viceversa, ovvero dimostriamo che preso $x \notin N(A)$ esiste P ideale primo tale che $x \notin P$. Sia $S := \{x^n : n \in \mathbb{N}\}$ e si consideri la famiglia $\mathcal{I} := \{I \subsetneq A, I \text{ ideale}, I \cap S = \emptyset\}$. Siccome $x \notin N(A)$, $\mathcal{I}$ contiene (0) e quindi $\mathcal{I}$ è una famiglia non vuota. Si consideri l'ordine $\subseteq$ sugli elementi di $\mathcal{I}$. Con tale ordine $\mathcal{I}$ è un insieme parzialmente ordinato. Si verifica facilmente, come nella dimostrazione del teorema di Krull, che $(\mathcal{I}, \subseteq)$ è un insieme induttivo (ovvero ogni catena in $\mathcal{I}$ ha un elemento maggiorante). Per il lemma di Zorn esiste quindi un elemento massimale per $\mathcal{I}$. Chiamiamolo P. Chiaramente $x \notin P$; rimane solo da verificare che P è effettivamente un ideale primo, ovvero che per ogni $a, b \in A$ con $a, b \notin P$ si ha $ab \notin P$. Dato che $a, b \notin P$ allora $P + (a)$ e $P + (b)$ devono, per la massimalità di P in $\mathcal{I}$, intersecare S. Quindi esistono $n, m \in \mathbb{N}$, $p_1, p_2 \in P$, $h_1, h_2 \in A$ tali che $x^n = p_1 + ah_1$ e $x^m = p_2 + bh_2$. Ma allora $x^{n+m} = p_1p_2 + p_1bh_2 + p_2ah_1 + abh_1h_2$ cioè $x^{n+m} \in P + (ab)$, perciò necessariamente $ab \notin P$.

2. Siano A e B anelli commutativi unitari. Dimostrare che ogni ideale $Y \subseteq A \times B$ è del tipo $I \times J$ dove I è un ideale di A e J è un ideale di B.

   Soluzione:

   Chiaramente se I è ideale di A e J ideale di B allora $I \times J$ è un ideale di $A \times B$.

   Dimostriamo il viceversa. Sia Y ideale di $A \times B$. Sia $I := \{a \in A | \exists b \in B \text{ t.c. } (a, b) \in Y\}$ e sia $J :=:= \{b \in B | \exists a \in A \text{ t.c. } (a, b) \in Y\}$. I è ideale di A, infatti è non vuoto ($(0, 0) \in Y \Rightarrow 0 \in I$), è un sottogruppo (se $i_1, i_2 \in I$ allora esistono $b_1, b_2 \in B$ tali che $(i_1, b_1) \in Y$ e $(i_2, b_2) \in Y$, da cui $(i_1 - i_2, b_1 - b_2) \in Y \Rightarrow i_1 - i_2 \in I$) ed è chiuso per il prodotto con elementi di A ($(a, 1)(i_1, b_1) = (ai_1, b_1) \in Y \Rightarrow ai_1 \in I$). Analogamente J è un ideale. Dato che ovviamente $Y \subseteq I \times J$, rimane solo da verificare che $I \times J \subseteq Y$. Sia $(i, j) \in I \times J$. Per definizione esistono $a \in A, b \in B$ tali che $(i, b), (a, j) \in Y$. Allora, dato che Y è un ideale, $(1, 0)(i, b) = (i, 0) \in Y$ e $(0, 1)(a, j) = (0, j) \in Y$, quindi anche $(i, j) = (i, 0) + (0, j) \in Y$.

3. Sia A un anello commutativo unitario e I, J ideali di A tali che $I+J=A$. Dimostrare che $\frac{A}{I\cap J} \cong \frac{A}{I} \times \frac{A}{J}$.

   Soluzione:

   Si consideri l'applicazione $\phi : A \to \frac{A}{I} \times \frac{A}{J}$ tale che $\phi(a) = (a+I, a+J)$. Si verifica facilmente che ϕ è un omomorfismo di anelli: $\forall a, b \in A$, $\phi(a+b) = (a+b+I, a+b+J) = (a+I, a+J) + (b+I, b+J) = \phi(a) + \phi(b)$ e $\phi(ab) = (ab+I, ab+J) = (a+I, a+J)(b+I, b+J) = \phi(a)\phi(b)$.

   Determiniamo il nucleo di ϕ: $\ker \phi = \{a \in A | a \in I, a \in J\} = I \cap J$.

   Dimostriamo che ϕ è suriettiva: siano $a+I \in \frac{A}{I}$ e $b+J \in \frac{A}{J}$. Dato che $I+J=A$ allora esistono $i \in I, j \in J$ tali che $i+j=1$. Consideriamo $aj+bi$. Si ha $aj = a(1-i) = a-ai$ e $bi = b-bj$, quindi $aj+bi+I = a+I$ e $aj+bi+J = b+J$, perciò $\phi(aj+bi) = (a+I, b+J)$.

   Applicando il teorema fondamentale di omomorfismo tra anelli segue dunque che $\frac{A}{I\cap J} \cong \frac{A}{I} \times \frac{A}{J}$.

4. Scomporre i seguenti interi di Gauss in prodotto di primi di Gauss:

$$7, 13, 1+3i, 5i-10;$$

   dimostrare poi che $\mathbb{Z}[i]/(1+2i)$ è un campo e calcolarne il numero degli elementi.

   Soluzione:

   Sia δ la norma euclidea standard definita a lezione. Dato che $x \in \mathbb{Z}[i]$ è invertibile se e solo se $\delta(x) = 1$ e che $\delta(7) = 49$ allora 7 è riducibile se e solo se 7 si può scrivere come prodotto di elementi di norma 7. In $\mathbb{Z}[i]$ non esistono, però, elementi di norma 7 ($7 \equiv 3 \mod 4$, quindi 7 non si può scrivere come somma di due quadrati) quindi 7 è irriducibile in $\mathbb{Z}[i]$.

   $13 = 4+9 = 2^2+3^2 = (2+3i)(2-3i)$. $\delta(2+3i) = \delta(2-3i) = 13$, che è un numero primo, perciò $2+3i$ e $2-3i$ sono elementi irriducibili, e quindi primi dato che $\mathbb{Z}[i]$ è un ED e in particolare un UFD.

   $\delta(1+3i) = 10$, quindi $1+3i$ o è irriducibile (primo) o è il prodotto di due elementi irriducibili di norma rispettivamente 2 e 5. Gli unici elementi di norma 2 in $\mathbb{Z}[i]$ sono $\pm 1 \pm i$; questi quattro interi di Gauss sono tutti associati tra loro, quindi è sufficiente studiare la divisibilità di $1+3i$ per, ad esempio, $1+i$. Concludendo: $1+3i = (1+i)(2+i)$.

   $5i-10 = 5(i-2) = (1+4)(i-2) = (1+2i)(1-2i)(i-2) = (1+2i)(1-2i)i(1+2i) = i(1+2i)^2(1-2i)$ e $1+2i$, $1-2i$ sono fattori primi dato che sono irriducibili poiché $\delta(1+2i) = \delta(1-2i) = 5$.

   Sia $I := (1+2i)$. Siccome $1+2i$ è irriducibile e $\mathbb{Z}[i]$ è un ED, e in particolare un PID, allora $(1+2i)$ è un ideale massimale e quindi $\mathbb{Z}[i]/I$ è un campo. Elenchiamone gli elementi. $\delta(1+2i) = 5$, quindi gli elementi distinti di $\mathbb{Z}[i]/I$, a parte $0+I$, si possono ricercare tra gli elementi del tipo $x+I$ con x di norma al più 4. Gli elementi di norma al più 4 sono: $\pm 1, \pm i, \pm 1 \pm i, \pm 2, \pm 2i$. Però $1-(-1+i) = 2-i = -i(1+2i) \in I$, quindi $1+I = -1+i+I$. Analogamente $-1-(1-i) = -2+i = i(1+2i) \in I$, $i-(-1-i) = 1+2i \in I$, $-i-(1+i) = -2i-1 = -(1+2i) \in I$,

$1-(-2i) = 1+2i \in I$, $-1-(2i) = -1-2i \in I$, $i-2 = i(1+2i) \in I$, $-i-(-2) = -i+2 = -i(1+2i) \in I$. Inoltre $1+I$, $-1+I$, $i+I$, $-i+I$ sono tutti elementi distinti di $\mathbb{Z}[i]/I$, dato che per ragioni di norma $1-(-1) = 2, 1-i, 1-(-i) = 1+i, -1-i, -1-(-i) = -1+i, i-(-i) = 2i$ non possono appartenere a I. Allora $\mathbb{Z}[i]/I = \{0+I, 1+I, -1+I, i+I, -i+I\}$ è un campo con 5 elementi.