Università degli Studi Roma Tre
Anno Accademico 2009/2010
AL2 - Algebra 2
Svogimento dell'esame di fine semestre

Es. 1. Cfr. Dikranjan, Aritmetica e Algebra, prop. 10.2.

Es. 2. Dimostreremo che A è un sottoanello unitario di $\mathbb{R}$ con le usuali operazioni. Essendo $\mathbb{R}$ commutativo seguirà che anche A è commutativo.

Prima di tutto verifichiamo che $(A,+)$ è un sottogruppo di $(\mathbb{R},+)$:
$\forall n,m,n',m' \in \mathbb{Z}$, $n+2m\sqrt{2}-(n'+2m'\sqrt{2}) = n-n'+2(m-m')\sqrt{2} \in A$.

Poi verifichiamo che A è chiuso per il prodotto:
$\forall n,m,n',m' \in \mathbb{Z}$, $(n+2m\sqrt{2})(n'+2m'\sqrt{2}) = nn'+8mm'+2(m'n+mn')\sqrt{2} \in A$.

Infine concludiamo, osservando che l'unità di $\mathbb{R}$, cioè 1, appartiene anche ad A.

Es. 3. $\mathbb{Z}[\sqrt{-6}] = \{a+b\sqrt{-6} | a,b \in \mathbb{Z}\}$ e per ogni $a,b \in \mathbb{Z}$ la norma $N(a+b\sqrt{-6}) := a^2+6b^2$.

Come visto a lezione, gli elementi invertibili di $\mathbb{Z}[\sqrt{-6}]$ sono tutti e soli gli elementi di norma 1. Quindi, nel nostro caso, solamente ± 1.

Inoltre in $\mathbb{Z}[\sqrt{-6}]$ non vi possono essere elementi di norma 5, dato che 5 non è un quadrato. Questo implica che gli elementi di norma 25 sono forzatamente irriducibili, dato che $\forall x,y \in \mathbb{Z}[\sqrt{-6}]$, $N(xy) = N(x)N(y)$ e quindi se un elemento di norma 25 si scrive come prodotto di altri due elementi, allora necessariamente uno dei due deve avere norma 1, quindi deve essere invertibile.

$25 = 5 \cdot 5$ ma si ha anche $25 = (1+2\sqrt{-6})(1-2\sqrt{-6})$ con $5, 1+2\sqrt{-6}, 1-2\sqrt{-6}$ irriducibili, dato che $N(5) = N(1+2\sqrt{-6}) = N(1-2\sqrt{-6}) = 25$. Inoltre 5 e $1+2\sqrt{-6}$ o $1-2\sqrt{-6}$ non sono associati, dato che gli unici invertibili di $\mathbb{Z}[\sqrt{-6}]$ sono ± 1. Quindi, avendo scritto due distinte fattorizzazioni di 25 in elementi irriducibili, possiamo concludere che $\mathbb{Z}[\sqrt{-6}]$ non è un UFD.

Es. 4. Per ogni $f(X), g(X) \in \mathbb{Z}[X]$, $\Psi(f(X)+g(X)) = \Psi((f+g)(X)) = (f+g)(3) \mod 8 = f(3) \mod 8 + g(3) \mod 8 = \Psi(f(X)) + \Psi(g(X))$. Inoltre per ogni $f(X), g(X) \in \mathbb{Z}[X]$, $\Psi(f(X)g(X)) = \Psi((fg)(X)) = (fg)(3) \mod 8 = (f(3) \mod 8) \cdot (g(3) \mod 8) = \Psi(f(X))\Psi(g(X))$. Quindi Ψ è effettivamente un omomorfismo di anelli.

Ψ è suriettivo, dato che per ogni $k \mod 8 \in \mathbb{Z}_8$ si ha $\Psi(k) = k \mod 8$.

Per il teorema fondamentale di omomorfismo di anelli allora $\mathbb{Z}[X]/\ker\Psi \cong \mathbb{Z}_8$. Siccome $\mathbb{Z}[X]$ è un anello commutativo unitario e $\mathbb{Z}_8$ non è un dominio di integrità (ad esempio $(2 \mod 8) \cdot (4 \mod 8) = 0 \mod 8$, con $2 \mod 8$ e $4 \mod 8 \neq 0$), allora $\ker\Psi$ non può essere un ideale primo.

$\ker\Psi = \{f(X) | f(3) \equiv 0 \mod 8\}$. Dimostriamo che $\ker\Psi = \langle X-3, 8\rangle \subseteq \mathbb{Z}[X]$. Chiaramente $\langle X-3, 8\rangle \subseteq \ker\Psi$. Sia allora $f(X) \in \ker\Psi$. Dato che $X-3$ è monico, per il teorema di divisione con resto possiamo scrivere

$f(X) = (X-3)h(X) + r(X)$, con $r(X) = 0$ oppure $\deg(r(X)) = 0 \Rightarrow r(X) = r \in \mathbb{Z}$. Siccome $f(3) \equiv 0 \mod 8$ allora $r(3) = r \equiv 0 \mod 8$, cioè $r \in 8\mathbb{Z}$, quindi $f(X) \in \langle X-3, 8\rangle$.

Es. 5. Dimostreremo che A è un sottoanello di $\mathbb{Q}$. Infatti dato che $\forall \frac{n_1}{2^{\alpha_1}}, \frac{n_2}{2^{\alpha_2}} \in A$ si ha $\frac{n_1}{2^{\alpha_1}} - \frac{n_2}{2^{\alpha_2}} = \frac{2^{\alpha_2}n_1 + 2^{\alpha_1}n_2}{2^{\alpha_1+\alpha_2}} \in A$ allora $(A,+)$ è un sottogruppo di $(\mathbb{Q},+)$. Inoltre $(A,\cdot)$ è stabile: $\forall \frac{n_1}{2^{\alpha_1}}, \frac{n_2}{2^{\alpha_2}} \in A$ si ha $\frac{n_1}{2^{\alpha_1}} \cdot \frac{n_2}{2^{\alpha_2}} = \frac{n_1 n_2}{2^{\alpha_1+\alpha_2}} \in A$.

L'inclusione di A in $\mathbb{Q}$ è chiaramente un omomorfismo iniettivo. Inoltre per ogni $\frac{a}{b} \in \mathbb{Q}$, con $a, b \in \mathbb{Z}$, si ha $\frac{b}{2^0} \cdot \frac{a}{b} = \frac{a}{2^0}$: siccome $\frac{b}{2^0}$ e $\frac{a}{2^0} \in A$ allora $\mathbb{Q}$ è il campo dei quozienti di A.

Es. 6. Siano A, B anelli, $A, B \neq \{0\}$. Siano $a \in A, a \neq 0_A$, $b \in B, b \neq 0_B$. Allora $(a, 0_B), (0_A, b) \in A \times B$, $(a, 0_B), (0_A, b) \neq (0_A, 0_B) = 0_{A\times B}$ ma $(a, 0_B) \cdot (0_A, b) = (0_A, 0_B)$, quindi $(a, 0_B)$ e $(0_A, b)$ sono divisori dello zero.

Es. 7. $\langle 2, X\rangle \neq \mathbb{Z}[X]$, dato che $1 \notin \langle 2, X\rangle$ (tutti i polinomi in $\langle 2, X\rangle$ hanno termine noto divisibile per 2).

Se $\langle 2, X\rangle$ fosse principale, allora $\exists f(X) \in \mathbb{Z}[X]$ tale che $\langle 2, X\rangle = \langle f(X)\rangle$. Quindi, in particolare, $2 \in \langle f(X)\rangle$ e $X \in \langle f(X)\rangle$, cioè $\exists h(X), k(X) \in \mathbb{Z}[X] \setminus \{0\}$ tali che $2 = f(X)h(X)$ e $X = f(X)k(X)$. Siccome $\mathbb{Z}$ è un dominio, allora $0 = \deg(2) = \deg(f(X)) + \deg(h(X))$, da cui $f(X) = c \in \mathbb{Z}$, con $c \neq \pm 1$, altrimenti $\langle f(X)\rangle = \mathbb{Z}[X]$. Quindi $X = ck(X)$, assurdo, perché X ha contenuto 1 mentre $ck(X)$ ha contenuto divisibile per c.

Siccome $\langle 2, X\rangle$ non è un ideale principale, allora $\mathbb{Z}[X]$ non è un PID e quindi $\mathbb{Z}[X]$ non può essere neanche un dominio euclideo, dato che $ED \Rightarrow PID$.

Es. 8. Il polinomio ha coefficienti in $\mathbb{Z}$ ed è primitivo (perché monico), quindi è irriducibile in $\mathbb{Q}$ se, e solo se, è irriducibile in $\mathbb{Z}$. Dato che il polinomio è primitivo, e il numero primo 3 ne divide tutti i coeff., salvo il coeff. direttore e, in aggiunta, $3^2 = 9$ non divide il termine noto 12, allora per il criterio di Eisenstein $X^4 + 6X + 12$ è irriducibile in $\mathbb{Z}[X]$ e quindi in $\mathbb{Q}[X]$.

Es. 9. $\mathbb{F}_7$ è un campo e $X^2 + 1$ un polinomio di secondo grado privo di radici in $\mathbb{F}_7$, quindi $X^2 + 1$ è irriducibile in $\mathbb{F}_7[X]$. $\mathbb{F}_7$ è un campo e quindi $\mathbb{F}_7[X]$ è un dominio euclideo e, in particolare, un PID. Dato che $X^2 + 1$ è irriducibile allora l'ideale da esso generato è massimale e quindi l'anello quoziente è un campo K.

Per il teorema di Kronecker $K = \{a_0 + a_1\alpha | a_0, a_1 \in \mathbb{F}_7, \alpha^2 + 1 = 0\}$ e $\{1, \alpha\}$ è una base di K su $\mathbb{F}_7$. Allora $|K| = 7^2 = 49$.