UITWERKING TENTAMEN ALGEBRA 2
22-12-2011.

① a) We passen het algoritme van Euclides toe.

$$\frac{5+5i}{2+3i} = \frac{(5+5i)(2-3i)}{13} = \frac{25-5i}{13} = 2 + \frac{-1}{13} - \frac{5}{13}i,$$

$$5+5i = 2(2+3i) + (1-i), \qquad 1-i = 5+5i - 2(2+3i)$$

$$\frac{2+3i}{1-i} = \frac{(2+3i)(1+i)}{2} = \frac{-1+5i}{2} = 2i + \left(-\tfrac{1}{2} + \tfrac{1}{2}i\right)$$

$$2+3i = 2i(1-i) + i = 2i\{5+5i - 2(2+3i)\} + i$$

Dus

$$(1+4i)(2+3i) - 2i(5+5i) = i, \Rightarrow$$
$$\boxed{(4-i)(2+3i) - 2(5+5i) = 1}$$

b) Zijn $\alpha, \beta \in \mathbb{Z}[i]$ de getallen uit a). Dan kunnen we als oplossing $x = \beta(5+5i) - \alpha(2+3i)$ nemen, omdat $\beta(5+5i) \equiv 1 \pmod{2+3i}$, $-\alpha(2+3i) \equiv 1 \pmod{5+5i}$. Dit geeft

$$x = (-2)\cdot(5+5i) - (4-i)(2+3i) = -2(5+5i) - \{1 - (-2)(5+5i)\}$$
$$= -4(5+5i) - 1 = \boxed{-21 - 20i}$$

② a) In $\mathbb{F}_2[X]$ geldt:
$X^4+3X^3+5X^2+6X+7 = X^4+X^3+X^2+1$.
Deze is deelbaar door $X+1$ (wl. 1 is een nulpunt). Dus

$$X+1 \;|\; X^4+X^3+X^3+1 \;\mid\; X^3+X+1$$
$$\underline{X^4+X^3}$$
$$X^3+1$$
$$\underline{X^3+X}$$
$$X+1$$
$$\underline{X+1}$$
$$0$$

$X^4+X^3+X^3+1 = (X+1)(X^3+X+1)$

X^3+X+1 is irreducibel in $\mathbb{F}_2[X]$ want het heeft geen nulpunten in $\mathbb{F}_2$

Dus $\boxed{X^4+3X^3+5X^2+6X+7 = (X+1)(X^3+X+1) \text{ in } \mathbb{F}_2[X]}$

In $\mathbb{F}_2[X]$ geldt:
$X^4+3X^3+5X^2+6X+7 = X^4+2X^2+1 = (X^2+1)^2$
X^2+1 is reducibel in $\mathbb{F}_2[X]$ (geen nulpunt)

Dus $\boxed{X^4+3X^3+5X^2+6X+7 = (X^2+1)^2 \text{ in } \mathbb{F}_2[X]}$

$X^4+3X^3+5X^2+6X+7$ heeft geen lineaire factor in $\mathbb{Z}[X]$ (als niet in $\mathbb{F}_2[X]$) en ook geen kwadratische factor (als niet in $\mathbb{F}_2[X]$)
Dus $X^4+3X^3+5X^2+6X+7$ is $\boxed{\text{irreducibel in } \mathbb{Z}[X]}$

b) We passen het criterium van Eisenstein toe:
Zij R een ontwikkelingsring, en $f(X) = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n$ met $p \nmid a_0$, $p \mid a_1, \dots, p \mid a_{n-1}$, $p \mid a_n$ en $p^2 \nmid a_n$ voor zeker irreducibel element p van R. Dan is f irreducibel in $R[X]$.
We nemen in dat geval $R = \mathbb{C}[X_2]$. Er geldt:
$X_1^3 + X_2^3 + 1 = X_1^3 + (X_2+1)(X_2^2 - X_2 + 1)$. Bijvoorbeeld X_2+1 is irreducibel in $\mathbb{C}[X_2]$,
dus $X_1^3 + X_2^3 + 1$ is $\boxed{\text{irreducibel in } \mathbb{C}[X_2][X_1] = \mathbb{C}[X_1, X_2]}$

c) We bewijzen met inductie naar n dat $X_1^3 + X_2^3 + \dots + X_n^3 + 1$ irreducibel is in $\mathbb{C}[X_1, \dots, X_n]$. Voor $n=2$ hebben we dat net bewezen. Pas Eisenstein toe met $R = \mathbb{C}[X_2, \dots, X_n]$, $f = X_2^3 + \dots + X_n^3 + 1$.
Volgens de inductie-aanname is f irreducibel in R.
Dus $X_1^3 + (X_2^3 + \dots + X_n^3 + 1)$ is $\boxed{\text{irreducibel in } \mathbb{C}[X_2, \dots, X_n][X_1] = \mathbb{C}[X_1, \dots, X_n]}$

(3) We berekenen eerst $(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_2+\alpha_3)$. Omdat $\alpha_1+\alpha_2+\alpha_3 = S_1$ is dit gelijk aan $(S_1-\alpha_3)(S_1-\alpha_2)(S_1-\alpha_1) = f(S_1) = S_1^3 - S_1^3 + S_1S_2 - S_3 = S_1S_2 - S_3$. Verder is

$$\left(X - \frac{1}{\alpha_1+\alpha_2}\right)\left(X - \frac{1}{\alpha_2+\alpha_3}\right)\left(X - \frac{1}{\alpha_1+\alpha_3}\right) = X^3 - t_1X^2 + t_2X - t_3,$$

met

$$t_1 = \frac{1}{\alpha_1+\alpha_2} + \frac{1}{\alpha_2+\alpha_3} + \frac{1}{\alpha_1+\alpha_3} = \frac{(\alpha_2+\alpha_3)(\alpha_1+\alpha_3) + (\alpha_1+\alpha_2)(\alpha_1+\alpha_3) + (\alpha_1+\alpha_2)(\alpha_2+\alpha_3)}{S_1S_2 - S_3}$$

$$= \frac{\alpha_3^2 + S_2 + \alpha_1^2 + S_2 + \alpha_2^2 + S_2}{S_1S_2 - S_3} = \frac{\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 3S_2}{S_1S_2 - S_3}$$

$$= \frac{S_1^2 - 2S_2 + 3S_2}{S_1S_2 - S_3} = \frac{S_1^2 + S_2}{S_1S_2 - S_3}$$

$$t_2 = \frac{1}{(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)} + \frac{1}{(\alpha_1+\alpha_2)(\alpha_2+\alpha_3)} + \frac{1}{(\alpha_1+\alpha_3)(\alpha_2+\alpha_3)} = \frac{\alpha_2+\alpha_3 + \alpha_1+\alpha_3 + \alpha_1+\alpha_2}{S_1S_2 - S_3}$$

$$= \frac{2S_1}{S_1S_2 - S_3}$$

$$t_3 = \frac{1}{(\alpha_1+\alpha_2)(\alpha_1+\alpha_3)(\alpha_2+\alpha_3)} = \frac{1}{S_1S_2 - S_3}.$$

(4) a) Stel $\alpha = a+b\sqrt{15}$, $\beta = c+d\sqrt{15}$. Dan is
$\alpha\beta = (a+b\sqrt{15})(c+d\sqrt{15}) = ac+15bd + (ad+bc)\sqrt{15}$. Er geldt:

$$N(\alpha\beta) = (ac+15bd)^2 - 15(ad+bc)^2 = a^2c^2 + 30abcd + 15^2b^2d^2 - 15a^2d^2 - 30abcd - 15b^2c^2$$
$$= a^2c^2 + 15^2b^2d^2 - 15(a^2d^2 + b^2c^2)$$

en $N(\alpha)N(\beta) = (a^2-15b^2)(c^2-15d^2) = a^2c^2 + 15^2b^2d^2 - 15(a^2d^2+b^2c^2)$
$= N(\alpha\beta)$

Sneller: zij $\alpha' = a-b\sqrt{15}$, $\beta' = c-d\sqrt{15}$. Dan is $\alpha'\beta' = (\alpha\beta)' =$
$ac+15bd - (ad+bc)\sqrt{15}$. Bijgevolg:
$N(\alpha\beta) = \alpha\beta\cdot(\alpha\beta)' = (\alpha\alpha')(\beta\beta') = N(\alpha)N(\beta)$.

Zij $\alpha \in R$. Als $N(\alpha) = \pm 1$, dan is $\alpha\cdot\alpha' = \pm 1$,
dus $\alpha^{-1} = \pm\alpha' \in R$, $\alpha \in R^*$.
Stel $\alpha \in R^*$. Dan is er een $\beta \in R$ met $\alpha\beta = 1$. Dus $N(\alpha)N(\beta) = N(1) = 1$.
Omdat $N(\alpha) \in \mathbb{Z}$ geldt dat $N(\alpha) = \pm 1$.

b) Beschouw $R \to \mathbb{F}_3$: $a+b\sqrt{15} \mapsto a \pmod 3$. Dit is een surjectief ringhomomorfisme, namelijk
$(a+b\sqrt{15})(c+d\sqrt{15}) = ac+15bd+(ad+bc)\sqrt{15}$ beeldt af op
$ac \pmod 3$, en $0,1,2 \in R$ beelden af op de restklassen
$0 \pmod 3$, $1 \pmod 3$, $2 \pmod 3$.
De kern van dit homomorfisme is
$\{a+b\sqrt{15} : a \equiv 0 \pmod 3\} = (3, \sqrt{15})$. Dus $R/(3,\sqrt{15}) \cong \mathbb{F}_3$ is een lichaam, en $(3,\sqrt{15})$ is een maximaal ideaal.

Stel $(3,\sqrt{15})$ is een hoofdideaal, zeg (α). Dan is $\alpha \mid 3$,
dus $N(\alpha) \mid N(3) = 9$, en $\alpha \mid \sqrt{15}$, dus $N(\alpha) \mid N(\sqrt{15}) = 15$.
Bijgevolg, $N(\alpha) \mid 3$. Maar er zijn geen elementen van norm ± 3.
Dus $\alpha \in R^*$. Maar $(3,\sqrt{15}) \subsetneq R$

b) (vervolg) $(3,\sqrt{15})^2 = (3,\sqrt{15})(3,\sqrt{15}) = (3^2, 3\sqrt{15}, 15)$
$= (3, 3\sqrt{15}) = (3)$

c) Er geldt $15 = \sqrt{15}\cdot\sqrt{15} = 3\cdot 5$
We leiden nu dat $3, 5$ en $\sqrt{15}$ irreducibel zijn in R, en dat 3 en 5 niet geassocieerd zijn. Dan volgt dat R **geen** ontbindingsring is
Stel 3 is reducibel. Dan is er $\alpha \in R$ met $\alpha \mid 3$, α geen eenheid, en α niet geassocieerd met 3. Dus $N(\alpha) \mid N(3) = 9$ en $N(\alpha) = \pm 3$. Maar er zijn in R geen elementen van norm ± 3. Op precies dezelfde manier volgt dat 5 en $\sqrt{15}$ irreducibel zijn. Verder is $N(5) \mid N(3) = 25/9 \neq \pm 1$, dus 5 en 3 zijn niet geassocieerd in R.

d) Merk op dat $4+\sqrt{15} \in R^*$ omdat $N(4+\sqrt{15}) = 4^2 - 15\cdot 1^2 = 1$.
$4+\sqrt{15}$ is geen eenheidswortel, dus het heeft oneindige orde, maw $(4+\sqrt{15})^n$ $(n \in \mathbb{Z})$ zijn alle verschillend. Dus R^* is zeker **oneindig**

(5) a) f is duidelijk additief. Verder geldt en injectief.
$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ = eenheidsmatrix, en

$$f((a+bi)(c+di)) = f(ac-bd+(ad+bc)i)$$

$$= \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} c & -d \\ d & c \end{pmatrix} = f(a+bi)\,f(c+di)$$

voor $a+bi, c+di \in \mathbb{Z}[i]$. Dus f is een ringhomomorfisme.

b) In ieder geval wordt M voortgebracht over $\mathbb{Z}$, dus zeker over $\mathbb{Z}[i]$, door $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
Verder is

$$i\cdot\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad i\cdot\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Dus M wordt voortgebracht over $\mathbb{Z}[i]$ door $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ en $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
We laten nu zien dat dit een basis van M over $\mathbb{Z}[i]$ geeft. Er geldt

$$(a+bi)\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (c+di)\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\cdot\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \text{ en dat is } 0 \iff a=b=c=d=0$$

Dus $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ zijn lineair onafhankelijk over $\mathbb{Z}[i]$.

c) N is duidelijk gesloten onder optelling. We laten nu dat N gesloten is onder vermenigvuldiging met $\mathbb{Z}[i]$. Er geldt voor $a+bi \in \mathbb{Z}[i]$, $\begin{pmatrix} x & x \\ z & z \end{pmatrix} \in N$,

$$(a+bi)\begin{pmatrix} x & x \\ z & z \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}\begin{pmatrix} x & x \\ z & z \end{pmatrix} = \begin{pmatrix} ax-bz & ax-bz \\ bx+az & bx+az \end{pmatrix} \in N$$

Tenslotte is $\begin{pmatrix} x & x \\ z & z \end{pmatrix} = (x+iz)\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Dus N wordt voortgebracht door $\boxed{\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}}$. $\begin{pmatrix} i & i \\ 0 & 0 \end{pmatrix}$ is geen horde-element.

d) Beschouw de afbeelding

$$g: M \to \mathbb{Z}[i]: \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mapsto x - y + i(z - w)$$

Deze afbeelding is additief en surjectief. Verder geldt voor $a+bi \in \mathbb{Z}[i]$:

$$g((a+bi)\begin{pmatrix} x & y \\ z & w \end{pmatrix}) = g\left(\begin{pmatrix} ax - bz & ay - bw \\ bx + az & by + aw \end{pmatrix}\right)$$

$$= a(x-y) - b(z-w) + i(b(x-y) + a(z-w)) = (a+bi)(x - y + i(z-w))$$
$$= (a+bi)\, g\left(\begin{pmatrix} x & y \\ z & w \end{pmatrix}\right).$$

Dus g is een surjectief $\mathbb{Z}[i]$-module-isomorfisme.
Er geldt:

$$\ker g = \left\{\begin{pmatrix} x & y \\ z & w \end{pmatrix} : x = y,\ z = w\right\} = N.$$

Dus $M/N \cong \mathbb{Z}[i]$ wegens de isomorfiestelling voor modulen.

Andere methode: $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right\}$ is een $\mathbb{Z}[i]$-basis van M volgens b). Dus $\left\{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$ is ook een $\mathbb{Z}[i]$-basis van M. Bijgevolg:

$$M = \mathbb{Z}[i]\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \mathbb{Z}[i]\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = N \oplus \mathbb{Z}[i]\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

en dus

$$M/N \cong \mathbb{Z}[i] \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cong \mathbb{Z}[i].$$

□