Algebraic number theory

Solutions sheet 1

January 25, 2011

1. (i) Since $\alpha^3 = 5$, the ring $\mathbb{Z}[\alpha]$ is the set of integral linear combinations of 1, α, α^2. This gives an isomorphism of $\mathbb{Z}$-modules $\mathbb{Z}^3 \tilde{\longrightarrow} \mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]$ is a free $\mathbb{Z}$-module. In the basis 1, α, α^2 the element $\alpha + \alpha^2$ acts as the matrix

$$\begin{pmatrix} 0 & 5 & 5 \\ 1 & 0 & 5 \\ 1 & 1 & 0 \end{pmatrix}$$

Computing its characteristic polynomial we get $f(x) = x^3 + 25x - 30$.

(ii) The same method gives $f(x) = x^4 - 10x^2 - 20x + 20$.

2. $\frac{1}{2}(1 + \sqrt{d})$ is the root of $x^2 - x - \frac{1}{4}(1 - d) = 0$, a monic polynomial with integral coefficients.

3. Let $a \in A$, $a \neq 0$. Then $a^{-1} \in R$, since R is a field. Since a^{-1} is integral over A, we have

$$a^{-n} + a_{n-1}a^{-(n-1)} + \ldots + a_1 a^{-1} + a_0 = 0, \text{ for some } a_i \in A,$$

hence

$$a^{-1} = -(a_{n-1} + \ldots + a_1 a^{n-2} + a_0 a^{n-1}) \in A.$$

4. The field of fractions of $F[x]$ is the set $F(x)$ of rational functions $\frac{f(x)}{g(x)}$, where $f(x)$ and $g(x)$ are in $F[x]$, and $g(x)$ is not the zero polynomial. Write our element as the fraction in lowest terms. If $g(x)$ is not a constant polynomial, we deduce a contradiction by using the same proof as in class.

5. (i) The $F[x^2]$-module $F[x]$ is generated by 1 and x. Now Thm. 3.2 implies that every element of $F[x]$ is integral over $F[x^2]$.

(ii) Write $f(x) = g(x^2) + xh(x^2)$ for some polynomials $g(x)$ and $h(x)$. Then $f(x)$ is a root of $t^2 - 2g(x^2)t + g(x^2)^2 - x^2h(x^2)^2 = 0$, a monic polynomial with coefficients in $F[x^2]$.

6. To prove that A is a ring it is enough to check that A is closed under $+$, $-$ and $\times$, and $1 \in A$, which is straightforward. The field of fractions of A is $F(x)$, because $x = \frac{x^3}{x^2}$, and x^2, x^3 are both in A. Now x is a root of the monic polynomial $t^2 - x^2$ with coefficients in A (since $x^2 \in A$), so x is an element of $F(x)$ which is integral over A, but $x \notin A$. Hence A is not integrally closed. In fact, $F[x]$ is generated by 1 and x as an A-module, so any element of $F[x]$ is integral over A, by Thm. 3.2. From Q4 we see that $F[x]$ is integrally closed, so it must be the integral closure of A.

7. Let $x \in \tilde{F}$, $x \neq 0$. There exist $a_0, \ldots, a_{n-1} \in F$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0.$$

If $a_0 = 0$ we can divide by x, so we can assume that $a_0 \neq 0$. Then

$$x^{-1} = -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) \in \tilde{F}.$$