Solutions to Problem Set 7

1) Let $f(x,y) = \prod_{a \in \mathbb{F}_q}(x+ay)$, and then I claim that the element $y \in \mathbb{F}_q[x,y]/(f)$ cannot be integral over $\mathbb{F}_q[x+a_0y]$ for any $a_0 \in \mathbb{F}_q$. Indeed, otherwise we would have a relation of the form:

$$y^n + \sum_{i=0}^{n-1} y^i \cdot g_i(x+a_0y) = 0 \mod \prod_{a \in \mathbb{F}_q}(x+ay)$$

where g_i are certain single variable polynomials with coefficients in $\mathbb{F}_q$. Taking the constant coefficients of the polynomials g_i, we would obtain a monic polynomial in y that is divisible by $x+a_0y$, which is impossible.

2) Let $K = \text{Frac } R$ denote the fraction field. We claim that:

$$K = \mathbb{C}(t) \qquad \text{where} \qquad t = \frac{x}{y}$$

Indeed, $x = t^4$ and $y = t^3$ due to the relation $x^3 = y^4$, which means that we have a surjective homomorphism $K \to \mathbb{C}(t)$. But since K is a field, this is an isomorphism.

Under the identification $K = \mathbb{C}(t)$, the ring R corresponds to $\mathbb{C}[t^3, t^4]$, and so it is contained in $\mathbb{C}[t]$. Since $\mathbb{C}[t]$ is integral over R (e.g. the relation $t^4 - x = 0$) and $\mathbb{C}[t]$ is integrally closed in $\mathbb{C}(t)$ (by analogy with the way we showed integers are integrally closed in the rationals), we conclude that the normalization of R is $\mathbb{C}[t]$.

3) We will prove the statement by induction on the degree of f. Suppose $f = gh$ where $g, h \in R'[x]$, and consider the ring $A_1 = R'[x]/(g)$. Since g is monic, we have $R' \subset A_1$. By construction, the polynomial g has a root inside A, so we may write:

$$g(x) = (x - \alpha_1)g_1(x)$$

with $g_1 \in A_1[x]$ monic. We repeat the procedure by constructing the ring $A_2 = A_1[x]/(g_1)$ and so on, until after $\deg f$ iterations of this procedure, we will have an extension:

$$R \subset R' \subset A$$

such that $g(x) = (x - \alpha_1)...(x - \alpha_l)$ and $h(x) = (x - \beta_1)...(x - \beta_l)$ inside the ring A. Each α_i and β_j are integral over R, since they are roots of $f \in R[x]$. But then so are any expression in the α's and β's, including the coefficients of g and h.

4) Suppose the set of algebraic integers (i.e. those $c \in \mathbb{C}$ which are integral over $\mathbb{Z}$) is generated by $c_1, ..., c_n$. Let us consider minimal polynomials:

$$(x - c_{i,1})...(x - c_{i,k_i}) \in \mathbb{Q}[x] \qquad \text{where} \qquad c_{i,1} = c_i$$

for all i. Then for any integers $k_1, ..., k_n$, we have:

$$\prod_{\text{where } s_i \text{ goes over } \{1,...,k_i\}}^{(s_1,...,s_n)} (x - k_1 c_{1,s_1} - k_2 c_{2,s_2} - ... - k_n c_{n,s_n}) \in \mathbb{Q}[x]$$

because the coefficients of the left hand side are symmetric functions in $\{c_{i,1}, ..., c_{i,k_i}\}$ for all i. This would imply that any algebraic integer has a minimal polynomial of degree $\leq k_1...k_n$ over $\mathbb{Q}$, which is absurd, since we could take for example a root of the poynomial $x^{k_1...k_n+1} - 2$ (which is irreducible by Eisenstein's criterion).