Solutions to Homework 9

Math 600, Fall 2007

42 (10 points) Dummit-Foote, 9.1 #9: $R[x_1, x_2, \cdots]$ has ideals which are not finitely generated.

Consider the ideal I of polynomials with constant term being zero. Suppose $I = (p_1, p_2, \cdots, p_m)$ is finitely generated. By renumbering the indeterminates, we know that the p_i are polynomials in $R[x_1, x_2, \cdots x_n]$ for some positive integer n. Clearly, the monomials x_i for $i > n$ are in I but not in $(p_1, p_2, \cdots, p_m) \subset R[x_1, x_2, \cdots]$. This contradiction shows that I cannot be finitely generated.

43 (10 points) Dummit-Foote, 9.1 #13: Prove that $F[x,y]/(y^2 - x)$ and $F[x,y]/(y^2 - x^2)$ are not isomorphic rings for any field F.

The ring $F[x,y]/(y^2 - x)$ is isomorphic to $F[y]$ by the map sending $x \mapsto y^2$, $y \mapsto y$, and hence is an integral domain. But the ring $F[x,y]/(y^2 - x^2)$ is not a domain because $(y - x) \cdot (y + x) = 0$ with the factors non-zero.

44 (10 points) Dummit-Foote, 9.1 #17 (homogeneous ideal problem) Instruction given with the problem is straight-forward to carry out.

45 (10 points): For all primes p, give the factorization of $X^4 + 1$ in $\mathbb{F}_p[X]$.

$$
\begin{aligned}
x^4 + 1 = (x+1)^4 \text{ if } p &= 2 \\
x^4 + 1 = (x - \xi)(x - \xi^3)(x - \xi^5)(x - \xi^7) \text{ if } p &\equiv 1 \pmod 8 \text{ and } \xi \text{ is a primitive } 8^{\text{th}} \text{ root of unity} \\
x^4 + 1 = (x^2 - i)(x^2 + i) \text{ if } p &\equiv 5 \pmod 8 \text{ and } \iota \text{ is a primitive } 4^{\text{th}} \text{ root of unity} \\
x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \text{ if } p &\equiv 7 \pmod 8 \text{ and } \sqrt{2} \text{ is a square root of } 2 \\
x^4 + 1 = (x^2 + \sqrt{-2}x - 1)(x^2 - \sqrt{-2}x - 1) \text{ if } p &\equiv 3 \pmod 8 \text{ and } \sqrt{-2} \text{ is a square root of } -2
\end{aligned}
$$

The factorization for the case of the even prime is clear. The existence of a linear factor of $x^4 + 1$ is equivalent to the existence of a primitive 8^{th} root of unity in the field. If ξ is such a root, then ξ^3, ξ^5, ξ^7 are also roots. In view of the fact that $\mathbb{F}_p^\times$ is cyclic, the existence of such a ξ is equivalent to $8 \,|\, p - 1$. On the other hand if $p \equiv 5 \pmod 8$ then a primitive 4^{th} root of unity is available and the factorization given above follows. However if $p \equiv 3, 7 \pmod 8$ then we have to explicitly check for a factorization $x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)$. We obtain $b = d = 1$ if $a = \sqrt{2}$ exists and $b = d = -1$ if $a = \sqrt{-2}$ exists. Since -1 is a non-square for such p, one of these two possibilities always occurs (Again by cyclicity of $\mathbb{F}_p^\times$, the product of two non-squares is a square). Noting the fact from number theory that 2 is a square in $\mathbb{F}_p$ iff $p \equiv \pm 1 \pmod 8$ we obtain the last two equations.

46 (5 points): Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

Suppose, $\mathbb{Q}$ is a free $\mathbb{Z}$-module. Let v, w be two distinct basis elements. Then there should exist no nontrivial relation of the form $av + bw = 0$ with $a, b \in \mathbb{Z}$. However such a relation can always be found for $v, w \in \mathbb{Q}$. This contradiction shows that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

47 (10 points): We say a domain R (with fraction field F) is integrally closed provided that if $r \in F$ satisfies a monic polynomial in $R[X]$, then $r \in R$. Show that any UFD is integrally closed.

We have $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$ where the $a_i \in R$. Write $r = s/t$ with s and t being relatively prime. We rewrite the equation above as $s^n + a_{n-1}s^{n-1}t + \cdots + a_1 s t^{n-1} + a_0 t^n = 0$, which implies $t \mid s$. However t, s are relatively prime and hence t has to be a unit. Thus $r \in R$.

48 (10 points) Dummit-Foote, 10.3 #2: Show that $R^m \simeq R^n$ iff $n = m$

Let $\mathfrak{m}$ be a max'l ideal of R. The $R/\mathfrak{m}$-module $R^m/\mathfrak{m}R^m$ is isomorphic to $(R/\mathfrak{m})^m$. The isomorphism between R^m and R^n induces a vector space map from $(R/\mathfrak{m})^m$ to $(R/\mathfrak{m})^n$ which is easily shown to be bijective. Since $R/\mathfrak{m}$ is a field, we can use the theorem from linear algebra that isomorphic finite dimensional vector spaces have the same dimension to conclude $m = n$.