Selected Solutions to Homework 7

Tim Smits

5.2.14 Find the inverse of $[f(T)]$ in $F[T]/(p(T))$.

(a) $[2T-3]$ in $\mathbb{Q}[T]/(T^2-2)$

(b) $[T^2+T+1]$ in $(\mathbb{Z}/3\mathbb{Z})[T]/(T^2+1)$

Solution:

(a) We have $\mathbb{Q}[T]/(T^2-2) \cong \mathbb{Q}(\sqrt{2})$ via $[T] \to \sqrt{2}$, so this is equivalent to finding the inverse of $2\sqrt{2}-3$ in $\mathbb{Q}(\sqrt{2})$. We have $\frac{1}{2\sqrt{2}-3} = \frac{2\sqrt{2}+3}{-1} = -2\sqrt{2}-3$ by the usual method of rationalizing the denominator. Passing back through the isomorphism, this says $[2T-3]^{-1} = [-2T-3]$.

(b) We have $[T^2+1] = [0]$ in $(\mathbb{Z}/3\mathbb{Z})[T]/(T^2+1)$, so $[T^2+T+1] = [T]$. Note that since $[T^2] = [-1]$, this says $[T]^{-1} = [-T]$.

6.1.38 Let I be an ideal of a commutative ring R. Let $J = \{r \in R : r^n \in I \text{ for some } n\}$. Prove that J is an ideal of R containing I. (The ideal J is called the *radical* of I and is usually denoted as $\sqrt{I}$).

Solution: Let $a, b \in J$. Then $a^n \in I$ and $b^m \in I$ for some m, n. By the binomial theorem, $(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k}$. For $0 \leq k \leq n$, we have $b^{n+m-k} \in I$ so $\binom{n+m}{k} a^k b^{n+m-k} \in I$ because I is an ideal, and therefore absorbs multiplication. Similarly, for $n \leq k \leq n+m$ we have $a^k \in I$ so $\binom{n+m}{k} a^k b^{n+m-k} \in I$, and therefore $(a+b)^{n+m} \in I$ because I is closed under addition. This says $a+b \in J$. For $r \in R$, and $a \in J$ with $a^n \in I$, we have $(ra)^n = r^n a^n \in I$, so $ra \in J$. This says that J is an ideal of R. J clearly contains I, so we are done.

6.1.40 Prove that every ideal of $\mathbb{Z}$ is principal.

Solution: Let $I \subset \mathbb{Z}$ be an ideal. Choose $d \in I$ to be the minimal positive integer contained in I (which exists because $\mathbb{Z}$ is well-ordered). Clearly, we have $(d) \subset I$. For any $x \in I$, write $x = dq + r$ for some integers q, r with $0 \leq r < d$. Since $dq \in I$, this says $r = x - dq \in I$, so by definition of d we have $r = 0$. This says $x = dq$, so $I \subset (d)$ gives $I = (d)$ as desired.