Polynomial Rings

Tim Smits

1. (a) Prove that $\mathbb{Z}[T]$ and $\mathbb{Q}[T]$ are not isomorphic as rings.
   (b) Let R be a non-zero ring. Prove that $R[T]$ is not a field.
2. Compute the greatest common divisor of T^4+2T^2+2T+2 and $T^4+2T^3+T^2+2$ in $(\mathbb{Z}/3\mathbb{Z})[T]$.
3. Let F be a field. Prove there are infinitely many monic irreducible polynomials in $F[T]$.
4. Let $f \in \mathbb{Z}[T]$ be monic. Suppose that $a \in \mathbb{Q}$ is a root of f. Prove that $a \in \mathbb{Z}$.
5. Factor the following polynomials:
   (a) $T^3 + T + 1$ in $(\mathbb{Z}/3\mathbb{Z})[T]$
   (b) $T^4 + 1$ in $(\mathbb{Z}/5\mathbb{Z})[T]$
6. Find all irreducible polynomials of degree ≤ 4 in $(\mathbb{Z}/2\mathbb{Z})[T]$.
7. Prove the following polynomials are irreducible in $\mathbb{Q}[T]$:
   (a) $f(T) = 7T^4 + 6T^2 + 4T + 6$
   (b) $f(T) = \dfrac{T^p - 1}{T - 1} = 1 + T + \ldots + T^{p-1}$, for p prime. (Hint: look at $f(T+1)$)
8. Let R be a commutative ring.
   (a) Prove that $f \in R[T]$ is idempotent if and only if $f(T) = a$, where a is an idempotent in R.
   (b) Prove that $f \in R[T]$ is nilpotent if and only if all coefficients of f are nilpotent in R.

Solutions

1. (a) One of many different ways to see this: note that $\mathbb{Z}[T]$ has finitely many units (namely, ± 1) while $\mathbb{Q}[T]$ has infinitely many units (namely, $a \neq 0 \in \mathbb{Q}$). An isomorphism between these rings would induce a bijection on their units, which is impossible.

   (b) Suppose that $R[T]$ was a field. Then T would have an inverse, say $p(T) \in R[T]$. So $Tp(T) = p(T)T = 1$. Plugging in $T = 0$ would say that $0 = 1$ in R, so that R is the 0 ring, a contradiction.

2. Run the Euclidean algorithm:

$$\begin{aligned} T^4 + 2T^2 + 2T + 2 &= (T^4 + 2T^3 + T^2 + 2) \cdot 1 + (T^3 + T^2 + 2T) \\ T^4 + 2T^3 + T^2 + 2 &= (T^3 + T^2 + 2T)(T + 1) + (T^2 + T + 2) \\ T^3 + T^2 + 2T &= (T^2 + T + 2)(T) + 0 \end{aligned}$$

   So the greatest common divisor is $T^2 + T + 2$.

3. Suppose there were finitely many monic irreducibles, say $\pi_1, \ldots, \pi_k \in F[T]$. Consider $\pi = \pi_1 \cdots \pi_k + 1$. Then π must have an irreducible factor, since it's non-constant (which can be made monic by rescaling). However, notice that π is not divisible by any of π_i, since it leaves remainder of 1 upon division by π_i. This means there is a monic irreducible polynomial not on our list, a contradiction. Therefore, there are infinitely many monic irreducibles in $F[T]$.

4. Let $f(T) = T^n + \ldots + a_0 \in \mathbb{Z}[T]$ and suppose $a = \dfrac{r}{s}$ is a root of $f(T)$ in $\mathbb{Q}$. By the rational root theorem, $s \mid 1$ means $s = \pm 1$, so $a \in \mathbb{Z}$.

5. (a) $T^3 + T + 1$ is irreducible in $(\mathbb{Z}/3\mathbb{Z})[T]$ because it's a degree 3 polynomial with no root in $\mathbb{Z}/3\mathbb{Z}$.

   (b) Note that T^4+1 has no roots in $\mathbb{Z}/5\mathbb{Z}$, so it has no linear factors. Therefore, it if factors, we can write $T^4 + 1 = (T^2 + aT + b)(T^2 + cT + d)$ as a product of two irreducible quadratics, so we have $T^4 + 1 = T^4 + (a + c)T^3 + (ac + b + d)T^2 + (ad + bc)T + bd$. Comparing coefficients, we have $a + c = 0$, $ac + b + d = 0$, $ad + bc = 0$, and $bd = 1$. This means $c^2 = b + d$, $c(b - d) = 0$, and $bd = 1$. The last equation says $b = d = 1$ or $b = d = 4$, so the second equation is always satisfied and therefore we have $c^2 = 2$ or $c^2 = 3$ in $\mathbb{Z}/5\mathbb{Z}$. Neither of these are possible, so no such factorization exists. Therefore, $T^4 + 1$ is irreducible in $(\mathbb{Z}/5\mathbb{Z})[T]$.

6. If $f(T) \in (\mathbb{Z}/2\mathbb{Z})[T]$ is irreducible, it must have a constant term of 1 (otherwise it's divisible by T), and an *odd* number of non-zero terms. This is because if you have an *even* number of terms, then $f(1) = 0$ so $T + 1 \mid f(T)$.

   degree 1: Any degree one polynomial is irreducible: $T, T + 1$.
   degree 2: There is a single choice of polynomial that satisfies the conditions: $T^2 + T + 1$.
   degree 3:There are two choices of polynomials that satisfy our criterion: T^3+T^2+1, T^3+T+1.
   degree 4: There are four polynomials that could possibly work: $T^4 + T^3 + 1, T^4 + T + 1, T^4 + T^3 + T^2 + T + 1, T^4 + T^2 + 1$. Our criteria has ruled out having a linear factor, so we need to check if we have an irreducible quadratic factor. There is only one irreducible quadratic, and we see that $(T^2 + T + 1)^2 = T^4 + T^2 + 1$. Therefore, the irreducible degree 4 polynomials are $T^4 + T^3 + 1, T^4 + T + 1, T^4 + T^3 + T^2 + T + 1$.

7. (a) $f(T)$ is Eisenstein at 2, so is irreducible in $\mathbb{Q}[T]$.

   (b) We have $f(T + 1) = \dfrac{1}{T}((T + 1)^p - 1)$. By the binomial theorem, we have $(T + 1)^p = \displaystyle\sum_{k=0}^{p} \binom{p}{k} T^k$, so $f(T + 1) = \displaystyle\sum_{k=1}^{p} \binom{p}{k} T^{k-1}$. Note that $\dbinom{p}{k} = \dfrac{p!}{k!(p - k)!}$ is an integer that's divisible by p for $1 \leq k \leq p-1$, because none of factorials in the denominator contain a factor of p, since $1 \leq k, p-k < p$. The constant term of $f(T+1)$ is p, so by the Eisenstein criterion, $f(T+1)$ and therefore $f(T)$ are irreducible in $\mathbb{Q}[T]$.

8. (a) Suppose that $f(T) = a_nT^n + \ldots + a_0$ is idempotent. Then squaring says $f(T)^2 = f(T)$. By comparing the constant terms, we find that $a_0^2 = a_0$ so that a_0 is idempotent in R. By the way polynomial multiplication works, we can write $f(T)^2 = \sum_{k=0}^{2n} d_kT^k$ where $d_k = \sum_{i=0}^{k} a_ia_{k-i}$. Looking at the coefficient of T, we find $2a_0a_1 = a_1$. Multiplying by a_0 and using that $a_0^2 = a_0$, we get $2a_0a_1 = a_0a_1 \implies a_1a_0 = 0$. This means $a_1 = 0$. Looking at the coefficient of T^2, we have $d_2 = 2a_0a_2 + a_1^2 = a_2$, so $2a_0a_2 = a_2$ and the same argument shows that $a_2 = 0$. Now suppose that $a_k = 0$ for all $1, 2, \ldots, i$. Then $a_{k+1} = d_{k+1} = 2a_0a_{k+1}$, and repeating the argument says that $a_{k+1} = 0$. Therefore by induction, $a_n = 0$ for $n \geq 1$, so that $f(T) = a_0$ is a constant polynomial with a_0 idempotent in R. The backwards direction is obvious, so we're done.

   (b) Suppose that $f(T) = a_nT^n + \ldots + a_0$ is nilpotent. Then $f(T)^N = 0$ for some N. We have $f(T)^N = \sum_{k=0}^{nN} d_kT^k$ where $d_k = \sum_{i=0}^{k} a_ia_{k-i}$. The leading term of $f(T)^N$ is $a_n^NT^{nN}$, which equals 0, so $a_n^N = 0$ says a_n is nilpotent. Now consider $f(T) - a_nT^n$. Then $f(T) - a_nT^n$ is still nilpotent, because the difference of nilpotents is nilpotent, and $f(T) - a_nT^n$ has strictly smaller degree than $f(T)$. By inductively applying the above argument, we can conclude that $a_{n-1}, \ldots, a_0$ are all nilpotent. Conversely, suppose that $a_0, \ldots, a_n$ are nilpotent. Then clearly $a_0, a_1T, \ldots, a_nT^n$ are all nilpotent, and since sums of nilpotents are nilpotent, this says that $a_0 + \ldots + a_nT^n$ is nilpotent, so we're done.