ANALOGIES BETWEEN Z AND $F[T]$: HOMEWORK 0

KEITH CONRAD

Notational remark. The field of p elements, denoted $\mathbf{Z}_p$ in the first-year number theory course, will be denoted $\mathbf{F}_p$ in this course. This is a very standard notation.

Elementary number-theoretic functions. We begin by looking at functions on $\mathbf{F}_p[T]$ that are similar to those in elementary number theory on $\mathbf{Z}$.

1. For nonzero $h \in \mathbf{F}_p[T]$, we define the *norm* of h to be $\mathrm{N}h = p^{\deg h}$. This equals the number of polynomials modulo h, and is analogous to the usual absolute value on integers. (For a nonzero $m \in \mathbf{Z}$, $|m|$ equals the number of integers modulo m.) Prove $\mathrm{N}(h_1h_2) = (\mathrm{N}h_1)(\mathrm{N}h_2)$, and $\mathrm{N}h = 1$ if and only if h is a unit in $\mathbf{F}_p[T]$.

2. Let $\varphi_{\mathbf{F}_p[T]}(h)$ be the number of units in $\mathbf{F}_p[T]$ modulo h. For irreducible π, show

$$\varphi_{\mathbf{F}_p[T]}(\pi) = \mathrm{N}\pi - 1, \quad \varphi_{\mathbf{F}_p[T]}(\pi^k) = \mathrm{N}\pi^k - \mathrm{N}\pi^{k-1}.$$

Derive a general formula for $\varphi_{\mathbf{F}_p[T]}(h)$, in terms of the irreducible factorization of h, which is analogous to a classical formula for $\varphi(m) = \varphi_{\mathbf{Z}}(m)$. Compute $\varphi_{\mathbf{F}_7[T]}(4)$ and $\varphi_{\mathbf{F}_3[T]}(2T^5 + 2T^3 + T + 2)$.

3. Let $\tau_{\mathbf{F}_p[T]}(h)$ be the number of divisors of h in $\mathbf{F}_p[T]$, up to unit multiple. (That is, divisors which differ by a unit factor are counted as one divisor.) What is a formula for $\tau_{\mathbf{F}_p[T]}(h)$ in terms of the irreducible factorization of h? Compute $\tau_{\mathbf{F}_7[T]}(4)$ and $\tau_{\mathbf{F}_3[T]}(2T^5 + 2T^3 + T + 2)$.

4. Find the right definition of $\sigma_{\mathbf{F}_p[T]}(h)$, and justify your answer. Can you find any "perfect" polynomials in $\mathbf{F}_2[T]$ or $\mathbf{F}_3[T]$?

5. Define $\mu_{\mathbf{F}_p[T]}(h) = (-1)^r$ if $h = \pi_1 \cdots \pi_r$ is a product of r relatively prime irreducibles, and $\mu_{\mathbf{F}_p[T]}(h) = 0$ if h has a multiple irreducible factor.

a) Compute $\mu_{\mathbf{F}_2[T]}(T^3 + T)$.

b) How should you define $\mu_{\mathbf{F}_p[T]}(c)$ for nonzero $c \in \mathbf{F}_p$?

c) Prove a Möbius inversion formula on $\mathbf{F}_p[T]$.

d) For $p = 3, 5, 7, 11$, compute $\mu_{\mathbf{F}_p[T]}(T^q - 1)$ for many primes q. Observations?

6. Which of the functions $\varphi, \tau, \sigma, \mu$ can be defined on $\mathbf{Q}[T]$? On $\mathbf{R}[T]$? On $F[T]$?

Continued fractions. Let

$$F(T) := \left\{ \frac{a}{b} : a, b \in F[T], b \neq 0 \right\}.$$

These are the ratios of polynomials. Using the obvious rules for adding and multiplying, $F(T)$ is a field. Its elements are called *rational functions*. An example of a rational function which is not a polynomial is $T/(T^2 + 1)$.

Any $R \in F(T)$ can be expanded into a finite continued fraction using repeated division:

$$R = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}}},$$

where each a_n is in $F[T]$. For instance, repeated division in $\mathbf{F}_5[T]$ leads to the continued fraction

$$\frac{T^5+T^4+2T^3+1}{T^3+4T+3} = T^2+T+3+\cfrac{1}{2T+\cfrac{1}{T^2+4}}.$$

This procedure of repeated division will be said to produce the *standard* continued fraction for R. We write $R=[a_1,a_2,\ldots,a_m]$, with n-th convergent p_n/q_n determined by the same algorithm as in the integer case: $p_n = a_np_{n-1}+p_{n-2}$, and likewise for q_n, with the usual initial values $\left(\begin{smallmatrix} p_{-1} & p_0 \\ q_{-1} & q_0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

7. (Examples)

a) Expand each of the following rational functions into a standard continued fraction over $F(T)$ with $F=\mathbf{Q}$, $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_5$, $\mathbf{F}_7$, and $\mathbf{F}_{11}$:

$$\frac{T^4+T^2-T+1}{T^3+2T^2+T+7}, \quad \frac{T^4+T^2-T+1}{T^3+7T^2+T-3}.$$

b) For $p=2,3,5,7$, and 11, try to reduce mod p the entries $a_n \in \mathbf{Q}[T]$. (For instance, $1/4 \in \mathbf{Q}$ gets interpreted mod p as the inverse of 4.) Sometimes this can't be done, because a coefficient in $\mathbf{Q}$ has p in the denominator. How do the a_n's you already computed directly in $\mathbf{F}_p[T]$ seem to reflect such features over $\mathbf{Q}$?

8. (Identities, old and new)

a) Prove $p_nq_{n-1}-q_np_{n-1}=(-1)^n$ for $n \geq 0$.

b) Prove $p_nq_{n-2}-q_np_{n-2}=(-1)^{n-1}a_n$ for $n \geq 1$.

c) When $\deg a_n \geq 1$ for $n \geq 2$, prove $\deg(q_n)=\deg(a_nq_{n-1})$. (Try $n=2$ and 3 explicitly first.)

d) Prove the standard continued fraction of any $R \in F(T)$ satisfies $\deg a_n \geq 1$ for $n \geq 2$.

e) When $\deg a_n \geq 1$ for $n \geq 2$, prove $[a_1,\ldots,a_m]$ makes sense: the denominator is nonzero.

f) Let $R=[a_1,\ldots,a_m]$ be a standard continued fraction. For $n \leq m-1$, prove

$$R = \frac{p_n}{q_n} + \sum_{j=n+1}^{m} \frac{(-1)^{j+1}}{q_{j-1}q_j}.$$

This expresses the total finite continued fraction in terms of any convergent plus a sum of (exact) error terms.

9. (Uniqueness) If $[a_1,\ldots,a_r]=[b_1,\ldots,b_s]$ where $a_n, b_n \in F[T]$ and a_n, b_n are nonconstant for $n \geq 2$, prove $r=s$ and $a_n=b_n$ for all n. Show this uniqueness is false if we allow an entry beyond the first to be constant. (Examples?)

10. (Degree of rational functions) For nonzero polynomials f and g in $F[T]$, it is easy to see that

- $\deg(fg)=\deg f+\deg g$,
- $\deg(f \pm g) \leq \max(\deg f, \deg g)$,
- $\deg f \neq \deg g \Longrightarrow \deg(f \pm g)=\max(\deg f, \deg g)$.

The first property is log-like, and suggests how to extend the degree function to nonzero rational functions $R \in F(T)$: write $R=a/b$ with $a,b \in F[T]-\{0\}$ and set $\deg R = \deg a - \deg b$. For example, $1/(T+1)$ has degree -1 and $(T^2-1)/(-T^2+4)$ has degree 0 (a nonconstant rational function can have degree 0).

a) Show the degree on $F(T)-\{0\}$ is well-defined, *i.e.*, the value of $\deg R$ is independent of the way we write R as a ratio of polynomials.

b) Compute the degrees of $(T+1)/(-T^5+T)$, $1/(T^4+2)^3$, and $(T^3+T^2+T)/(T+1)$.

c) Check that the three properties of the degree on nonzero polynomials continue to hold on nonzero rational functions. Setting $\deg 0=-\infty$, with appropriate meaning given to addition with $-\infty$, show the properties also hold when one of f or g is 0.

d) For $c \in F$, $c \neq 0$, and $f \in F(T)$, show $\deg(f-c) < 0 \Longrightarrow \deg f = 0$. Give two examples of nonconstant f in $F(T)$ with $\deg(f-1) < 0$.

e) Let $R \in F(T)$ have standard continued fraction expansion $[a_1, \ldots, a_m]$. For $1 \leq n \leq m-1$, show

$$\deg\left(R - \frac{p_n}{q_n}\right) = -\deg(q_n q_{n+1}) = -\deg(a_{n+1} q_n^2),$$

using exercise 8f and properties of degrees. What is this equation analogous to in the classical theory of continued fractions? How is this stronger than the classical analogue?

11. (The polynomial analogue of the greatest integer) Writing $R = a/b$ as a ratio of *relatively prime* polynomials, let q be the quotient when a is divided by b, so $q \in F[T]$.

a) Show $\deg(R-q) < 0$, and q is the unique polynomial in $F[T]$ with this property. We call q the *polynomial part* of R, and write $q = \lfloor R \rfloor$. (For our purposes, elements of $F(T)$ with negative degree are interpreted as small, so this definition does resemble the usual greatest integer function.)

b) Compute $\lfloor R \rfloor$ for $R = (T^5 - 2T^3 + 3T^2 + 7T + 4)/(T^2 - 1)$ in $\mathbf{Q}(T)$ and in $\mathbf{F}_p(T)$ for $p = 2, 3, 5, 7, 11$. What is $\deg(R - \lfloor R \rfloor)$ in each case?

c) For the classical greatest integer function on $\mathbf{R}$, $\lfloor n + x \rfloor = n + \lfloor x \rfloor$ with $x \in \mathbf{R}$ and $n \in \mathbf{Z}$, and $\lfloor x/n \rfloor = \lfloor \lfloor x \rfloor / n \rfloor$ when $n \geq 1$. (Counterexample when $n < 0$?)

For $R \in F(T)$ and $h \in F[T]$, show $\lfloor h + R \rfloor = h + \lfloor R \rfloor$ and (for $h \neq 0$) $\lfloor R/h \rfloor = \lfloor \lfloor R \rfloor / h \rfloor$. Here are some properties which have no classical analogue: for $f, g \in F(T)$, $\lfloor f + g \rfloor = \lfloor f \rfloor + \lfloor g \rfloor$ and $\lfloor cf \rfloor = c \lfloor f \rfloor$, where $c \in F$. If $h \in F[T]$ is nonconstant, does $\lfloor R(h(T)) \rfloor = \lfloor R \rfloor (h(T))$?

12. (Pell's equation for polynomials) When $d > 1$ is a nonsquare integer, the equation $u^2 - dv^2 = 1$ has a solution in $\mathbf{Z}$ which is nontrivial ($v \neq 0$). It is found by the classical theory of infinite continued fractions. There are no nontrivial solutions in $\mathbf{Z}$ when $d < -1$. Let's now consider $u^2 - fv^2 = 1$ where $f = f(T)$ is a nonsquare in $F[T]$. We seek solutions (u, v) in $F[T]$ which are nontrivial (*i.e.*, $v \neq 0$).

a) Show $u^2 - (T^3 + 1)v^2 = 1$ has no nontrivial solution in $F[T]$. (Hint: Think about degrees.)

b) Show $u^2 - (2T^4 + T)v^2 = 1$ has no nontrivial solution in $\mathbf{F}_5[T]$. (Hint: Think about leading coefficients.)

c) Show $u^2 - 3v^2 = 1$ has a solution with nonzero $v \in \mathbf{F}_5$, but not with nonconstant $v \in \mathbf{F}_5[T]$.

d) Let $f \in F[T]$ be a nonsquare with $\deg f > 0$. If $u^2 - fv^2 = 1$ has a solution $u, v \in F[T]$ with $v \neq 0$, what conditions are forced on the degree and leading coefficient of f?

e) (Warm-up for the next part) Compute the continued fractions of $\sqrt{2}, \sqrt{5}$, and $\sqrt{10}$. Find the continued fraction for $\sqrt{m^2+1}$ when $m \geq 1$. Do likewise for $\sqrt{m^2-1}$ when $m \geq 2$ after testing $m = 2, 3, 4$.

f) Use your knowledge of the "parametrized" classical continued fractions in part e to find two solutions in $F[T]$ to each of the equations $u^2 - (T^2+1)v^2 = 1$ and to $u^2 - (T^2-1)v^2 = 1$, with $v \neq 0$.

Quadratic residues. Throughout this part, p is a fixed *odd* prime.

13. Let π be irreducible in $\mathbf{F}_p[T]$. Show the number of nonzero squares modulo π is $(\mathrm{N}\pi - 1)/2$.

14. For $f \not\equiv 0 \bmod \pi$, show $f \equiv \square \bmod \pi \iff f^{(\mathrm{N}\pi-1)/2} \equiv 1 \bmod \pi$.

15. For $f \in \mathbf{F}_p[T]$, define the Legendre symbol $\left(\frac{f}{\pi}\right)$ by

$$\left(\frac{f}{\pi}\right) = \begin{cases} 0, & \text{if } f \equiv 0 \bmod \pi, \\ 1, & \text{if } f \equiv \square \bmod \pi, f \not\equiv 0 \bmod \pi, \\ -1, & \text{if } f \not\equiv \square \bmod \pi. \end{cases}$$

Show $\left(\frac{f}{\pi}\right) \equiv f^{(\mathrm{N}\pi-1)/2} \bmod \pi$, $\left(\frac{fg}{\pi}\right) = \left(\frac{f}{\pi}\right)\left(\frac{g}{\pi}\right)$, and $\left(\frac{c}{\pi}\right) = \left(\frac{c}{p}\right)^{\deg \pi}$ for $c \in \mathbf{F}_p$. (Here $\left(\frac{c}{p}\right)$ is the usual Legendre symbol.)

16. Let $\pi = T^3 + 2T + 2$ in $\mathbf{F}_3[T]$. Compute $\left(\frac{f}{\pi}\right)$ when f is $T^2 + 2$, $2T^4 + T^3 + T$, and $2T^2 + T + 1$.

17. The definition of $(\frac{f}{\pi})$ in exercise 15 makes sense on $\mathbf{F}_2[T]$. Why is $(\frac{f}{\pi})$ uninteresting in this case?

Miscellaneous.

18. Let $f(X) \in \mathbf{Z}[X]$ be monic (that is, its leading coefficient is 1). Prove any rational root of $f(X)$ is an integer. What is the analogue in $F[T][X]$? Prove the polynomial $X^4+(T+1)X+T^8+T+2$ has no root in the field $\mathbf{F}_3(T)$.

19. Let $X^2 + bX + c \in F[X]$ have roots r and s: $X^2 + bX + c = (X - r)(X - s)$.

a) Prove $(r - s)^2 = b^2 - 4c$. Therefore $r \neq s \iff b^2 - 4c \neq 0$. In particular, when $2 = 0$ in F, $r \neq s \iff b \neq 0$.

b) When $2 \neq 0$ in F, completing the square simplifies the polynomial: $X^2 + bX + c = Y^2 - d$ where $Y = X + b/2$ and $d = b^2/4 - c$. When $2 = 0$ in F and the roots are *distinct*, give a change of variables so that $X^2 + bX + c = u^2(Y^2 + Y + d)$ for some $u, d \in F$ ($u \neq 0$) and variable Y. Show no linear change of variables transforms $X^2 + bX + c$ into $Y^2 - d$. (We regard $Y^2 + Y + d$, when $2 = 0$, as the "standard" form of quadratic polynomials with distinct roots, just as $Y^2 - d$ is when $2 \neq 0$.)

20. Suppose $2 \neq 0$ in F. For $g, h \in F[T]$ with $g^2 - h^2 \neq 0$, show

$$\deg(g^2 - h^2) \geq \max(\deg g, \deg h).$$