ANALOGIES BETWEEN Z AND $F[T]$: HOMEWORK 2

KEITH CONRAD

Squares.

1. Let F be a field not of characteristic 2 (i.e., $2 \neq 0$ in F), and f be a nonzero element of $F((1/T))$.

a) If f is a square in $F((1/T))$, prove f has even degree and its leading coefficient is a square in $F^\times$.

b) Suppose f has even degree and its leading coefficient is a square in $F^\times$. Prove f is a square in $F((1/T))$, by the method of successive approximations. (Let $\deg f = d = 2m$ and b^2 ($b \in F$) be the leading coefficient of f. Set $g_1 = bT^m$, so $\deg(f - g_1^2) \leq d - 1$. If $g_n \in F((1/T))$ satisfies $\deg(f - g_n^2) \leq d - n$, we can write $f - g_n^2 = c_n T^{d-n} + \cdots$, where $c_n \in F$. Find $a_n \in F$, in terms of c_n, such that $g_{n+1} := g_n + a_n T^{m-n}$ satisfies $\deg(f - g_{n+1}^2) \leq d - (n+1)$. Prove the sequence g_n converges in $F((1/T))$, and its limit is a square root of f.)

c) When f in part b has nonnegative degree, the sequence g_n starts off in $F[T]$. Prove that the last g_n which lies in $F[T]$ is the polynomial part of a square root of f. This gives an algorithm for computing polynomial parts of square roots.

d) For $f \in F((1/T))$ as in part b, prove the polynomial part $\lfloor \sqrt{f} \rfloor$ is the unique (up to sign) $g \in F[T]$ such that $\deg(f - g^2) < (\deg f)/2$. When $f(T) \in F[T]$ and $h(T) \in F[T]$ is nonconstant, does $\lfloor \sqrt{f(h(T))} \rfloor = \lfloor \sqrt{f} \rfloor (h(T))$?

e) Write a computer program to compute $\lfloor \sqrt{f} \rfloor$ when $f \in \mathbf{F}_p[T]$ ($p \neq 2$). As the first step, check there is a square root of f in $\mathbf{F}_p((1/T))$ by using the equivalent condition in part a.

2. Which of the following polynomials in $\mathbf{F}_7[T]$ have square roots in $\mathbf{F}_7((1/T))$? For each which does, compute one of its two square roots up to the $1/T^3$ term:

$$3T^2 + 5T + 1, \quad 4T^2 + 3, \quad T^3 + 2T + 1, \quad 2T^3 + T + 4, \quad T^4 + 6T^3 + T.$$

Is $(3T + 4)/(6T + 1)$ a square in $\mathbf{F}_7((1/T))$?

Continued fractions.

In the questions below, $\sqrt{f}$ (for monic $f \in F[T]$) is the square root with monic polynomial part.

3. Extend properties of the polynomial part on $F(T)$, as in exercise 11c of Homework 0, over to $F((1/T))$.

4. Let F be a field not of characteristic 2. Compute (standard) continued fractions for $\sqrt{T^2 + 1}$ and $\sqrt{T^2 - 1}$ in $F((1/T))$. Compare to the continued fractions for the real numbers $\sqrt{m^2 + 1}$ and $\sqrt{m^2 - 1}$ when $m \geq 2$. Solve exercise 12f on Homework 0 using continued fractions in $F((1/T))$.

5. Use continued fractions in $\mathbf{Q}((1/T))$ to find a nontrivial solution to $u^2 - (T^2 + 3T + 1)v^2 = 1$ in $\mathbf{Q}[T]$, and then find two more nontrivial solutions. Generalize your work to $u^2 - (T^2 + bT + c)v^2 = 1$ in $F[T]$, where F does not have characteristic 2 and the discriminant $b^2 - 4c \in F$ is nonzero.

6. Compute the continued fraction for $\alpha = \sqrt{T^4 + 2T^3 + T}$ in $\mathbf{F}_{23}((1/T))$. Then find a solution to $u^2 - (T^4 + 2T^3 + T)v^2 = 1$ in $\mathbf{F}_{23}[T]$ where both u and v are nonconstant. Verify the equality

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{|a_{n+1} q_n^2|}$$

for $n = 1, 2, 3, 4$. Find the best rational approximation to α having a denominator with degree at most 5 and then with degree at most 6.

7. In Homework 0, exercise 7b, the continued fraction of a rational function over $\mathbf{Q}$ and of its reductions over various $\mathbf{F}_p$ had a peculiar relationship when $a_n \in \mathbf{Q}[T]$ could not be reduced mod p. Instead, look at the mod p reductions of the convergents $p_n/q_n \in \mathbf{Q}(T)$. (First rescale so all coefficients are integral.) How do these compare with the intrinsic mod p convergents?

8. This exercise examines the continued fraction for $\sqrt{T^4 - 8T - 8}$.

a) Compute the first six a_n in $\mathbf{Q}((1/T))$ and the entire periodic sequence $\{a_n\}$ in $\mathbf{F}_7((1/T))$. Does behavior like that in the previous exercise occur here?

b) Solve $u^2 - (T^4 - 8T - 8)v^2 = 1$ nontrivially in $\mathbf{F}_7[T]$.

c) If you have suitable computer assistance, repeat this in $\mathbf{F}_p((1/T))$ for all odd primes up to 23.

9. Let F be a field not of characteristic 2. For $b, c \in F[T]$ such that $b^2 - 4c \notin F$, assume the equation $u^2 + buv + cv^2 = 1$ has a solution $u, v \in F[T]$ with $v \neq 0$. Prove $x^2 + bx + c$ has roots in $F((1/T))$ and u/v is a convergent to the continued fraction of one of these roots.

Quadratic residues.

10. Fix an odd prime p. For $c \in \mathbf{F}_p$ and $f(T) \in \mathbf{F}_p[T]$, show $(\frac{f(T)}{T-c}) = (\frac{f(c)}{p})$, where the first Legendre symbol is defined on $\mathbf{F}_p[T]$ and the second Legendre symbol is the classical one. What is $(\frac{2T^2-T+3}{T-2})$ in $\mathbf{F}_5[T]$?

11. Read the handout on roots and irreducible polynomials through the end of section 3, if you have not already done so. For $p \neq 2$, let π be irreducible in $\mathbf{F}_p[T]$. Let α be a root of π in a field $E \supset \mathbf{F}_p$.

a) Prove $(\frac{T}{\pi}) = \alpha^{(\mathrm{N}\pi - 1)/2}$.

b) When π is monic, use part a to prove $(\frac{T}{\pi}) = (-1)^{\frac{p-1}{2} \deg \pi}(\frac{\pi(0)}{p})$. (Hint: $(\mathrm{N}\pi - 1)/2 = (1 + p + p^2 + \cdots + p^{d-1})(p-1)/2$, where $d = \deg \pi$. Express $\pi(0)$ in terms of the roots of π.)

12. ($p = 2$, continued) Solvability of the quadratic congruence

$$x^2 + (T+1)x + T^5 + T \equiv 0 \bmod T^3 + T^2 + 1$$

in $\mathbf{F}_2[T]$ is equivalent to the vanishing of what symbol $[f, \pi)$? Likewise with

$$x^2 + (T^2 + T + 1)x + 1 \equiv 0 \bmod T^3 + T^2 + 1.$$

Nonunique factorization.

13. Let $d \in \mathbf{Z}$ be a nonsquare and p be an odd prime.

a) Prove: if p or $-p$ has the form $u^2 - dv^2$ ($u, v \in \mathbf{Z}$), then $(\frac{d}{p}) = 1$.

b) Prove the converse to part a under the assumption that $\mathbf{Z}[\sqrt{d}]$ has unique factorization. (If $p | n^2 - d$, show p is not irreducible in $\mathbf{Z}[\sqrt{d}]$. The case $d = -1$ is the Gaussian integers.)

c) Since $\mathbf{Z}[\sqrt{3}]$ has a division algorithm, it has unique factorization. Thus, part b says $(\frac{3}{p}) = 1 \Longrightarrow p$ or $-p$ has the form $u^2 - 3v^2$. Make the conclusion explicit for $p = 11$.

d) When $d = -5, -10, -22, 10, 79$, or 122, show the converse to part a fails for some p (*i.e.*, $(\frac{d}{p}) = 1$ and neither p nor $-p$ has the form $u^2 - dv^2$). Therefore such rings $\mathbf{Z}[\sqrt{d}]$ do not have unique factorization, but this was not proved by finding examples of nonunique factorization!

14. Let $p \neq 2$, $f \in \mathbf{F}_p[T]$ be a nonsquare, and π be irreducible in $\mathbf{F}_p[T]$.

a) Prove: if, for some $a \in \mathbf{F}_p^\times$, $a\pi$ has the form $u^2 - fv^2$ ($u, v \in \mathbf{F}_p[T]$), then $(\frac{f}{\pi}) = 1$.

b) Prove the converse to part a under the assumption that $\mathbf{F}_p[T][\sqrt{f}]$ has unique factorization. (Here $\sqrt{f}$ is a root of $X^2 - f$ in some field $E \supset \mathbf{F}_p(T)$. There may not be a square root of f in the particular field $\mathbf{F}_p((1/T))$, *e.g.*, when $f = T$.)

c) Prove $\mathbf{F}_p[T][\sqrt{f}]$ has unique factorization when $f = c$ is a constant (nonsquare) in $\mathbf{F}_p$ and also when $f = T$.

d) If $(\frac{T}{\pi}) = 1$, we now know $a\pi = u^2 - Tv^2$ for some $a \in \mathbf{F}_p^\times$ and $u, v \in \mathbf{F}_p[T]$. Make this conclusion explicit when $\pi = T^3 - T - 1 \in \mathbf{F}_3[T]$ and when $\pi = T^3 - 2 \in \mathbf{F}_7[T]$.

e) When $f = c$ is a constant nonsquare in $\mathbf{F}_p$, show the role of a in parts a and b can be discarded: if a unit multiple of π has the form $u^2 - cv^2$ $(u, v \in \mathbf{F}_p[T])$, then π also has this form.

f) Check part b applies to the irreducibles $2T^2 + T + 1$ and $T^4 + 2T^3 + 2$ in $\mathbf{F}_3[T]$, using $f = 2$. Then write each one in the form $u^2 - 2v^2$ $(u, v \in \mathbf{F}_3[T])$.

g) Prove $\mathbf{F}_p[T][\sqrt{T^3 - T}]$ does not have unique factorization by finding an irreducible π in $\mathbf{F}_p[T]$ such that $(\frac{T^3-T}{\pi}) = 1$ and $a\pi \neq u^2 - (T^3 - T)v^2$ for any $a \in \mathbf{F}_p^\times$ and $u, v \in \mathbf{F}_p[T]$. (This can be done with $\deg \pi \leq 2$, in fact with $\deg \pi = 1$ for $p > 3$ if you are clever enough.)

15. Let $f \in \mathbf{F}_2[T]$ not be $\wp(g) = g^2 + g$ for any $g \in \mathbf{F}_2[T]$, and π be irreducible in $\mathbf{F}_2[T]$.

a) Prove: if $\pi = u^2 + uv + fv^2$ for some $u, v \in \mathbf{F}_2[T]$, then $[f, \pi) = 0$.

b) Prove the converse to part a under the assumption that $\mathbf{F}_2[T][\alpha]$ has unique factorization, where α satisfies $\alpha^2 + \alpha = f$.

c) Verify the assumption in part b holds when $f = 1$. Explain why it follows that every irreducible of even degree in $\mathbf{F}_2[T]$ must have the form $u^2 + uv + v^2$ $(u, v \in \mathbf{F}_2[T])$. Make such a representation explicit for $T^2 + T + 1$, $T^4 + T + 1$, $T^4 + T^3 + 1$, and $T^4 + T^3 + T^2 + T + 1$.

d) Show $T^2 + T + 1 \neq u^2 + uv + T^3v^2$ for any $u, v \in \mathbf{F}_2[T]$. What quadratic ring over $\mathbf{F}_2[T]$ therefore does not have unique factorization?

Miscellaneous.

16. When F is a field with characteristic $p > 0$ and $f \in F((1/T))$, show $\lfloor f^p \rfloor = \lfloor f \rfloor^p$. This will be useful later when $p = 2$ and $F = \mathbf{F}_2$. Try some examples.

17. Let F be a field with characteristic p. Show the polynomial $X^p - X + 1/T$ has a root in $F((1/T))$:

$$1 + \frac{1}{T} + \frac{1}{T^p} + \frac{1}{T^{p^2}} + \cdots .$$

What are the other roots? Show, on the other hand, that $X^p - X + T$ has no root in $F((1/T))$.

18. If $f(T), g(T) \in F[T]$ are squarefree, is $f(g(T))$ squarefree?

19. (Composition) For every $f(T) \in F((1/T))$, it makes sense to speak about $f(T^2), f(T^3)$, and so on as elements of $F((1/T))$. Does it make sense to speak about $f(h(T))$ where $h(T) \in F[T]$ is any nonconstant polynomial? What about $f(0)$? $f(1)$? $f(1/T)$?