SUMS OF SQUARES IN $\mathbf{Q}$ AND $\mathbf{F}(T)$

KEITH CONRAD

1. Introduction

To illustrate the analogies between integers and polynomials, we prove a theorem about sums of squares over $\mathbf{Z}$ and then prove an analogous result in $F[T]$ (where F does not have characteristic 2). Specifically, we will show that if an integer is a sum of 2 or 3 rational squares then it is in fact a sum of 2 or 3 integer squares. The polynomial analogue is stronger: if a polynomial is a sum of n squares of rational functions for any n then it is a sum of n squares of polynomials. The proof in the polynomial case is essentially the same as the integer case.

2. The integer case

Theorem 2.1. *If an integer is a sum of two rational squares then it is a sum of two integral squares. If an integer is a sum of three rational squares then it is a sum of three integral squares.*

Example 2.2. We have $193 = (1512/109)^2 + (83/109)^2$, $193 = (933/101)^2 + (1048/101)^2$, and $193 = 7^2 + 12^2$.

Example 2.3. We have $13 = (18/11)^2 + (15/11)^2 + (32/11)^2$, $13 = (2/3)^2 + (7/3)^2 + (8/3)^2$, and $13 = 0^2 + 3^2 + 2^2$.

Proof. Suppose $v = (s_1, s_2) \in \mathbf{Q}^2$ satisfies $s_1^2 + s_2^2 = a$. We we will write this as $v \cdot v = a$. If s_1 and s_2 are in $\mathbf{Z}$, we're done, so we assume at least one of them is not in $\mathbf{Z}$. Write the s_i's with a common denominator: $s_i = m_i/d$ where the m_i's and d are in $\mathbf{Z}$ and $d \neq \pm 1$. We want to find a $w \in \mathbf{Q}^2$ such that $w \cdot w = v \cdot v$ and w has a common denominator of smaller size than v. Repeating this enough times, we will eventually get a common denominator of 1, meaning we have a as a sum of integer squares.

In $\mathbf{Z}$, divide each m_i by the common denominator d:

$$m_i = dq_i + r_i$$

where q_i and r_i are in $\mathbf{Z}$ and $|r_i| \leq d/2$. Since s_1 and s_2 are not both in $\mathbf{Z}$, some r_i is nonzero. Thus $v = (s_1, s_2) = \mathbf{q} + (1/d)\mathbf{r}$ where $\mathbf{q} = (q_1, q_2)$ and $\mathbf{r} = (r_1, r_2)$ are in $\mathbf{Z}^2$ and $\mathbf{r} \neq (0, 0)$.

Using the dot product,

$$v \cdot v = \left(\mathbf{q} + \frac{1}{d}\mathbf{r}\right) \cdot \left(\mathbf{q} + \frac{1}{d}\mathbf{r}\right) = \mathbf{q} \cdot \mathbf{q} + \frac{1}{d^2}\mathbf{r} \cdot \mathbf{r} + \frac{2}{d}\mathbf{q} \cdot \mathbf{r}. \tag{2.1}$$

Since $\mathbf{q}$ and $\mathbf{r}$ are integral vectors the dot products $\mathbf{q} \cdot \mathbf{q}$, $\mathbf{r} \cdot \mathbf{r}$, and $\mathbf{q} \cdot \mathbf{r}$ are in $\mathbf{Z}$. Since $|r_i| \leq d/2$, $\mathbf{r} \cdot \mathbf{r} = r_1^2 + r_2^2 \leq 2(d/2)^2 = d^2/2$, so $(1/d^2)\mathbf{r} \cdot \mathbf{r} \leq 1/2$.

Since $\mathbf{r} \neq \mathbf{0}$, we can consider the reflection $w = \tau_{\mathbf{r}}(v)$. From the properties of reflections, $w \cdot w = v \cdot v = a$. We will show the coordinates of $w \in \mathbf{Q}^2$ have a smaller common denominator than the common denominator d for v.

Explicitly,

$$\begin{aligned} w &= \tau_{\mathbf{r}}(v) \\ &= \tau_{\mathbf{r}}(\mathbf{q} + (1/d)\mathbf{r}) \\ &= \tau_{\mathbf{r}}(\mathbf{q}) - \frac{1}{d}\mathbf{r} \\ &= \left(\mathbf{q} - \frac{2\mathbf{q}\cdot\mathbf{r}}{\mathbf{r}\cdot\mathbf{r}}\mathbf{r}\right) - \frac{1}{d}\mathbf{r} \\ &= \mathbf{q} - \left(\frac{2\mathbf{q}\cdot\mathbf{r}}{\mathbf{r}\cdot\mathbf{r}} + \frac{1}{d}\right)\mathbf{r}. \end{aligned}$$

Multiplying (2.1) by $d/(\mathbf{r}\cdot\mathbf{r})$,

$$\frac{d(v\cdot v)}{\mathbf{r}\cdot\mathbf{r}} = \frac{d(\mathbf{q}\cdot\mathbf{q})}{\mathbf{r}\cdot\mathbf{r}} + \frac{1}{d} + \frac{2\mathbf{q}\cdot\mathbf{r}}{\mathbf{r}\cdot\mathbf{r}},$$

so

$$w = \mathbf{q} - \frac{d(v\cdot v - \mathbf{r}\cdot\mathbf{r})}{\mathbf{r}\cdot\mathbf{r}}\mathbf{r} = \mathbf{q} - \frac{v\cdot v - \mathbf{r}\cdot\mathbf{r}}{(\mathbf{r}\cdot\mathbf{r})/d}\mathbf{r},$$

where the denominator $(\mathbf{r}\cdot\mathbf{r})/d$ is an integer: by (2.1),

$$\frac{\mathbf{r}\cdot\mathbf{r}}{d} = d(v\cdot v - \mathbf{q}\cdot\mathbf{q}) - 2\mathbf{q}\cdot\mathbf{r}$$

and the right side is in $\mathbf{Z}$. We noted before that $(1/d^2)\mathbf{r}\cdot\mathbf{r} \leq 1/2$, so $(\mathbf{r}\cdot\mathbf{r})/d$ is at most $d/2 < d$, which means the common denominator for w is less than that for v, so we are done with the sum of two squares case.

The exact same proof works for a sum of three squares, using dot products and reflections in three dimensions instead of two dimensions. The only change to be made is the following: now we have $\mathbf{r} = (r_1, r_2, r_3)$ where $|r_i| \leq (1/2)d$, so $\mathbf{r}\cdot\mathbf{r} = r_1^2 + r_2^2 + r_3^2 \leq (3/4)d^2$ instead of $(1/2)d^2$. Now $(1/d^2)\mathbf{r}\cdot\mathbf{r} \leq 3/4$ instead of $1/2$, so $(\mathbf{r}\cdot\mathbf{r})/d \leq (3/4)d$ instead of $d/2$. This is still less than d, so everything still works in the proof when it is done for sums of three squares. □

Geometrically, we are looking at the circle $\{(x,y) : x^2 + y^2 = a\}$ and taking reflections of rational points through the nearest $\mathbf{Z}$-point to get new rational points.

The corresponding result for a sum of 2 cubes is false: $13 = (7/3)^3 + (2/3)^3$, but 13 is not a sum of two cubes in $\mathbf{Z}$ (look at how the cubes spread apart on the real line).

Theorem 2.1 has a nice application to the negative Pell equation. Pell's equation is $x^2 - dy^2 = 1$ for $d \in \mathbf{Z}$, and a famous result in number theory says for each $d > 1$ that's not a perfect square ($d = 2, 3, 5, 6, 7, 8, 10, 11, 12, \ldots$), the Pell equation $x^2 - dy^2 = 1$ has a solution (x, y) in positive integers.[1] The negative Pell equation is $x^2 - dy^2 = -1$, and there is a strong constraint on the d for which this equation admits an integral solution.

Corollary 2.4. *If $x^2 - dy^2 = -1$ has a solution in $\mathbf{Z}$ then d is a sum of two squares in $\mathbf{Z}$.*

Proof. If $x^2 - dy^2 = -1$ for $x, y \in \mathbf{Z}$, then $y \neq 0$. Since $dy^2 = x^2 + 1$, we have $d = (x/y)^2 + (1/y)^2$. That shows d is a sum of two rational squares, so d must also be a sum of two integral squares. □

[1] See https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn1.pdf and https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pelleqn2.pdf.

A further constraint on d in order for $x^2 - dy^2 = -1$ to be solvable in $\mathbf{Z}$ is that it has no prime factors that are 3 mod 4: necessarily $x^2 \equiv -1 \bmod d$, so if $p \mid d$ for prime p then $x^2 \equiv -1 \bmod p$, and it's known that -1 is not a square mod p for primes $p \equiv 3 \bmod 4$.[2] However, there are d with no prime factors that are 3 mod 4 and $x^2 - dy^2 = -1$ has no integral solution. The smallest two such squarefree d are 34 and 146. A longer list of such d is at `https://oeis.org/A031398`.

3. The polynomial analogue

Theorem 3.1. *Let $Q\colon F^n \to F$ be a non-degenerate n-dimensional quadratic form over a field F not of characteristic 2. If $v \in F(T)^n$ satisfies $Q(v) \in F[T]$ then there is some $w \in F[T]^n$ such that $Q(w) = Q(v)$. In other words, any polynomial that is represented by Q over $F(T)$ is represented by Q over $F[T]$.*

The quadratic form in this theorem has coefficients in F, not simply in $F[T]$. For example, the 1-dimensional quadratic form $Q(x) = T^2x^2$ represents 1 over $F(T)$ but not over $F[T]$.

Proof. Let $v = (f_1, \ldots, f_n) \in F(T)^n$ satisfy $Q(v) \in F[T]$. Assume the f_i's are not all in $F[T]$. (Otherwise we are done.) Write the f_i's with a common denominator: $f_i = g_i/h$ where the g_i's and h are in $F[T]$ and h is non-constant. We want to find a $w \in F(T)^n$ such that $Q(w) = Q(v)$ and w has a common denominator of smaller degree than $\deg h$. Then repeating the argument will eventually produce a vector of polynomials $w \in F[T]^n$ such that $Q(w) = Q(v)$ and we're done.

In $F[T]$, divide each g_i by the common denominator h:

$$g_i = hq_i + r_i$$

where q_i and r_i are in $F[T]$ and $r_i = 0$ or $\deg r_i < \deg h$. Since not all f_i's are in $F[T]$, some r_i is nonzero. Thus $v = (f_1, \ldots, f_n) = \mathbf{q} + (1/h)\mathbf{r}$ where $\mathbf{q} = (q_1, \ldots, q_n)$ and $\mathbf{r} = (r_1, \ldots, r_n)$ are in $F[T]^n$ and $\mathbf{r} \neq (0, \ldots, 0)$.

Let B be the bilinear form associated to Q, so B has coefficients in F and

$$Q(v) = Q\left(\mathbf{q} + \frac{1}{h}\mathbf{r}\right) = Q(\mathbf{q}) + \frac{1}{h^2}Q(\mathbf{r}) + \frac{2}{h}B(\mathbf{q}, \mathbf{r}). \tag{3.1}$$

Since $\mathbf{q}$ and $\mathbf{r}$ are polynomial vectors and Q and B have coefficients in F, the values $Q(\mathbf{q})$, $Q(\mathbf{r})$, and $B(\mathbf{q}, \mathbf{r})$ are in $F[T]$. Since $\deg(r_ir_j) < 2\deg h$ or $r_ir_j = 0$, $Q(\mathbf{r})$ is 0 or $\deg Q(\mathbf{r}) < 2\deg h$. (Here we use the non-archimedean nature of the degree on $F[T]$, which has no analogue for the absolute value on $\mathbf{Z}$.)

We consider now two cases: $Q(\mathbf{r}) = 0$ and $Q(\mathbf{r}) \neq 0$.

If $Q(\mathbf{r}) = 0$ then $\mathbf{r}$ is a nonzero null vector for Q. Necessarily $n > 1$ (n is the dimension of Q), since Q is non-degenerate: a 1-dimensional quadratic form doesn't have any nonzero null vectors. We will find a nonzero constant vector $v_0 \in F^n$ such that $Q(v_0) = 0$. Then, since $n > 1$ and Q is non-degenerate, there is another null vector w_0 for Q in F^n with $B(v_0, w_0) = 1$. Then for any $f \in F[T]$, the polynomial vector $fv_0 + (1/2)w_0 \in F[T]^n$ satisfies

$$Q(fv_0 + (1/2)w_0) = f^2Q(v_0) + \frac{1}{4}Q(w_0) + 2B(fv_0, (1/2)w_0) = f,$$

showing Q is universal over $F[T]$. We are done.

[2]This leads to a second proof of Corollary 2.4, since primes that are not 3 mod 4 are known to be sums of two squares and the sums of two squares in $\mathbf{Z}^+$ are closed under multiplication.

To find such v_0, pull out the largest factor of T common to all the coordinates of $\mathbf{r}$: $\mathbf{r} = T^k(\mathbf{r}_0 + T\mathbf{r}_1)$, where $k \geq 0$, $\mathbf{r}_0 \in F^n$, $\mathbf{r}_0 \neq \mathbf{0}$, and $\mathbf{r}_1 \in F[T]^n$. Then

$$0 = Q(\mathbf{r}) = T^{2k}Q(\mathbf{r}_0 + T\mathbf{r}_1) = T^{2k}(Q(\mathbf{r}_0) + T^2Q(\mathbf{r}_1) + 2TB(\mathbf{r}_0, \mathbf{r}_1)).$$

Therefore $0 = Q(\mathbf{r}_0) + T^2Q(\mathbf{r}_1) + 2TB(\mathbf{r}_0, \mathbf{r}_1)$, Evaluating at $T = 0$ shows $\mathbf{r}_0 \in F^n$ is a null vector for Q. Use $v_0 = \mathbf{r}_0$.

Now suppose $Q(\mathbf{r}) \neq 0$. As in the situation over $\mathbf{Q}$, consider the reflection $w = \tau_{\mathbf{r}}(v)$. From the properties of reflections, $Q(w) = Q(v)$. We will show the coordinates of $w \in F(T)^n$ have a common denominator with smaller degree than the common denominator h for v.

Explicitly,

$$\begin{aligned} w &= \tau_{\mathbf{r}}(v) \\ &= \tau_{\mathbf{r}}(\mathbf{q} + (1/h)\mathbf{r}) \\ &= \tau_{\mathbf{r}}(\mathbf{q}) - \frac{1}{h}\mathbf{r} \\ &= \left(\mathbf{q} - \frac{2B(\mathbf{q}, \mathbf{r})}{Q(\mathbf{r})}\mathbf{r}\right) - \frac{1}{h}\mathbf{r} \\ &= \mathbf{q} - \left(\frac{2B(\mathbf{q}, \mathbf{r})}{Q(\mathbf{r})} + \frac{1}{h}\right)\mathbf{r}. \end{aligned}$$

Multiplying (3.1) by $h/Q(\mathbf{r})$,

$$\frac{hQ(\mathbf{v})}{Q(\mathbf{r})} = \frac{hQ(\mathbf{q})}{Q(\mathbf{r})} + \frac{1}{h} + \frac{2B(\mathbf{q}, \mathbf{r})}{Q(\mathbf{r})},$$

so

$$w = \mathbf{q} - \frac{h(Q(v) - Q(\mathbf{r}))}{Q(\mathbf{r})}\mathbf{r} = \mathbf{q} - \frac{Q(v) - Q(\mathbf{r})}{Q(\mathbf{r})/h}\mathbf{r},$$

where the denominator $Q(\mathbf{r})/h$ is a polynomial: by (3.1),

$$\frac{Q(\mathbf{r})}{h} = h(Q(v) - Q(\mathbf{q})) - 2B(\mathbf{q}, \mathbf{r})$$

and the right side is in $F[T]$ (here, for the first time in the case when $Q(\mathbf{r}) \neq 0$, we use the assumption that $Q(v) \in F[T]$). The degree of $Q(\mathbf{r})/h$ is $\deg Q(\mathbf{r}) - \deg h < 2\deg h - \deg h = \deg h$, so we are done. □

Corollary 3.2. *If a polynomial in $F[T]$ is a sum of n squares in $F(T)$ then it is a sum of n squares in $F[T]$.*

Proof. Take $Q(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2$ in Theorem 3.1. □