SUMS OF SQUARES IN Q AND F(T)

KEITH CONRAD

1. Introduction

To illustrate the analogies between integers and polynomials, we prove a theorem about sums of squares over \( \mathbb{Z} \) 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 \( v = (s_1, s_2) \in \mathbb{Q}^2 \) satisfies \( s_1^2 + s_2^2 = a \). We will write this as \( v \cdot v = a \). If \( s_1 \) and \( s_2 \) are in \( \mathbb{Z} \), we’re done, so we assume at least one of them is not in \( \mathbb{Z} \). Write the \( s_i \)'s with a common denominator: \( s_i = m_i/d \) where the \( m_i \)'s and \( d \) are in \( \mathbb{Z} \) and \( d \neq \pm 1 \). We want to find a \( w \in \mathbb{Q}^2 \) 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 \( \mathbb{Z} \), divide each \( m_i \) by the common denominator \( d \):

\[ m_i = dq_i + r_i \]

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

Using the dot product,

\[ v \cdot v = (q + \frac{1}{d} r) \cdot (q + \frac{1}{d} r) = q \cdot q + \frac{1}{d^2} r \cdot r + \frac{2}{d} q \cdot r. \]

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

Since \( r \neq 0 \), we can consider the reflection \( w = \tau_r(v) \). From the properties of reflections, \( w \cdot w = v \cdot v = a \). We will show the coordinates of \( w \in \mathbb{Q}^2 \) have a smaller common denominator than the common denominator \( d \) for \( v \).
Explicitly,
\[
  w = \tau r(v) \\
  = \tau r(q + (1/d)r) \\
  = \tau r(q) - \frac{1}{d} r \\
  = \left(q - \frac{2q \cdot r}{r \cdot r}\right) - \frac{1}{d} r \\
  = q - \left(\frac{2q \cdot r}{r \cdot r} + \frac{1}{d}\right)r.
\]

Multiplying (2.1) by \(d/(r \cdot r)\),
\[
\frac{d(v \cdot v)}{r \cdot r} = \frac{d(q \cdot q)}{r \cdot r} + \frac{1}{d} + \frac{2q \cdot r}{r \cdot r},
\]
so
\[
w = q - \frac{d(v \cdot v - r \cdot r)}{r \cdot r} = q - \frac{v \cdot v - r \cdot r}{(r \cdot r)/d} r,
\]
where the denominator \((r \cdot r)/d\) is an integer: by (2.1),
\[
\frac{r \cdot r}{d} = \frac{d(v \cdot v - q \cdot q) - 2q \cdot r}{r \cdot r},
\]
and the right side is in \(\mathbb{Z}\). We noted before that \((1/d^2)r \cdot r \leq 1/2\), so \((r \cdot r)/d\) 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 \(r = (r_1, r_2, r_3)\) where \(|r_i| \leq (1/2)d\), so \(r \cdot r = r_1^2 + r_2^2 + r_3^2 \leq (3/4)d^2\) instead of \((1/2)d^2\). Now \((1/d^2)r \cdot r \leq 3/4\) instead of \(1/2\), so \((r \cdot r)/d \leq (3/4)d\) 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 \(\mathbb{Z}\)-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 \(\mathbb{Z}\) (look at how the cubes spread apart on the real line).

3. The polynomial analogue

**Theorem 3.1.** Let \(Q : F^n \to F\) 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 \( v = (f_1, \ldots, f_n) = q + (1/h)r \) where \( q = (q_1, \ldots, q_n) \) and \( r = (r_1, \ldots, r_n) \) are in \( F[T]^n \) and \( r \neq (0, \ldots, 0) \).

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

\[
(3.1) \quad Q(v) = Q(q) + \frac{1}{h^2}Q(r) + \frac{2}{h}B(q, r).
\]

Since \( q \) and \( r \) are polynomial vectors and \( Q \) and \( B \) have coefficients in \( F \), the values \( Q(q), Q(r), \) and \( B(q, r) \) are in \( F[T] \). Since \( \deg(r_ir_j) < 2 \deg h \) or \( r_ir_j = 0 \), \( Q(r) \) is 0 or \( \deg Q(r) < 2 \deg h \). (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: \( Q(r) = 0 \) and \( Q(r) \neq 0 \).

If \( Q(r) = 0 \) then \( r \) 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 \( f v_0 + (1/2)w_0 \in F[T]^n \) satisfies

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

showing \( Q \) is universal over \( F[T] \). We are done.

To find such \( v_0 \), pull out the largest factor of \( T \) common to all the coordinates of \( r \):

\[
r = T^k(r_0 + Tr_1),
\]

where \( k \geq 0 \), \( r_0 \in F^n \), \( r_0 \neq 0 \), and \( r_1 \in F[T]^n \). Then

\[
0 = Q(r) = T^{2k}Q(r_0 + Tr_1) = T^{2k}(Q(r_0) + T^2Q(r_1) + 2TB(r_0, r_1)).
\]

Therefore \( 0 = Q(r_0) + T^2Q(r_1) + 2TB(r_0, r_1) \). Evaluating at \( T = 0 \) shows \( r_0 \in F^n \) is a null vector for \( Q \). Use \( v_0 = r_0 \).

Now suppose \( Q(r) \neq 0 \). As in the situation over \( Q \), consider the reflection \( w = \tau_r(v) \).

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,

\[
w = \tau_r(v) = \tau_r(q + (1/h)r) = \tau_r(q) - \frac{1}{h}r = \left( q - \frac{2B(q, r)}{Q(r)} \right) - \frac{1}{h}r = q - \left( \frac{2B(q, r)}{Q(r)} + \frac{1}{h} \right) r.
\]
Multiplying (3.1) by $h/Q(r)$,
\[
\frac{hQ(v)}{Q(r)} = \frac{hQ(q)}{Q(r)} + \frac{1}{h} + \frac{2B(q,r)}{Q(r)},
\]
so
\[
w = q - \frac{h(Q(v) - Q(r))}{Q(r)} r = q - \frac{Q(v) - Q(r)}{Q(r)/h} r,
\]
where the denominator $Q(r)/h$ is a polynomial: by (3.1),
\[
\frac{Q(r)}{h} = h(Q(v) - Q(q)) - 2B(q,r)
\]
and the right side is in $F[T]$ (here, for the first time in the case when $Q(r) \neq 0$, we use the assumption that $Q(v) \in F[T]$). The degree of $Q(r)/h$ is $\deg Q(r) - \deg h < 2 \deg h - \deg h = \deg h$, 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. \qed