Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 35 (1989)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: AN ELEMENTARY PROOF OF A THEOREM ON QUADRATIC FORMS OVER THE RATIONAL NUMBERS

Autor: Leep, David B.

Kapitel: §1. Reductions to prove the Main Theorem

DOI: https://doi.org/10.5169/seals-57371

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 19.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

the classical integral theory of quadratic forms over the integers and also depends on Dirichlet's theorem or Gauss' theory mentioned above. A third way is to use the so called weak Hasse-Minkowski theorem. A proof of this can be found in [La], p. 174-178, but knowledge is required of Witt rings, local fields, exact sequences, and Springer's theory for quadratic forms over local fields.

Until now, no proof of the Main Theorem, much less an elementary one, has appeared exploiting the fact that $D_{\mathbf{Q}}(\langle 1, a, b, ab\rangle)$ is a multiplicative subgroup of $\mathbf{Q}^\times$. We present a truly elementary proof below using nothing more exotic than the notion of quadratic residues and the Möbius function.

We follow basic terminology and notation as found in [La]. In particular, a quadratic form $\langle a_1, ..., a_n\rangle$ is isotropic over F if there exist $x_1, ..., x_n \in F$, not all zero, such that $\sum_{i=1}^{n} a_i x_i^2 = 0$. We have the orthogonal sum $\langle a_1, ..., a_m\rangle \perp \langle b_1, ..., b_n\rangle = \langle a_1, ..., a_m, b_1, ..., b_n\rangle$ and $\langle\langle a, b\rangle\rangle$ stands for $\langle 1, a, b, ab\rangle$.

I wish to thank T.Y. Lam for the proof of Proposition 1.4 which is much simpler than my original proof.

§ 1. Reductions to prove the Main Theorem

1.1. Main Theorem. *Let* $a, b \in \mathbf{Q}^\times$. *Then*

$$D_{\mathbf{Q}}(\langle 1, a, b, ab\rangle) = \begin{cases} \mathbf{Q}^\times_{>0} & \text{if } a, b > 0 \\ \mathbf{Q}^\times & \text{otherwise}. \end{cases}$$

We begin by stating some basic results needed to prove Theorem 1.1.

1.2. Lemma. *Let* $q = \langle a_1, ..., a_n\rangle$, $a_i \in F^\times$.

(a) *If* q *is isotropic over* F, *then* $D_F(q) = F^\times$.

(b) *Let* $c \in F^\times$. *Then* $q \perp \langle c\rangle$ *is isotropic over* F *if and only if* $-c \in D_F(q)$.

Proof. (a) Let $c \in F^\times$ be given. An appropriate linear change of variable lets us assume $q(1, 0, ..., 0) = 0$. Then

$$q(x_1, ..., x_n) = x_1\left(\sum_{i=2}^{n} b_i x_i\right) + Q(x_2, ..., x_n)$$

where some $b_i \neq 0$. Choose $a_2, ..., a_n \in F$ such that $\sum_{i=2}^{n} b_i a_i \neq 0$ and let

$a_1 = \dfrac{c - Q(a_2, ..., a_n)}{b_2 a_2 + ... + b_n a_n}$. Then $q(a_1, a_2, ..., a_n) = c$.

(b) Suppose $q(a_1, ..., a_n) + ca_{n+1}^2 = 0$ where some $a_i \neq 0$. If $a_{n+1} \neq 0$, then $q\left(\dfrac{a_1}{a_{n+1}}, ..., \dfrac{a_n}{a_{n+1}}\right) = -c$. If $a_{n+1} = 0$, then q is isotropic and (a) implies $-c \in D_F(q)$. The converse is trivial.

1.3. LEMMA. *Let* $a, b \in F^\times$. *Then* $D_F(\langle\langle a, b\rangle\rangle)$ *is a subgroup of* $F^\times$.

Proof. Clearly $1 \in D_F(\langle\langle a, b\rangle\rangle)$ and the following formula shows $D_F(\langle\langle a, b\rangle\rangle)$ is closed under multiplication.

$$\begin{aligned}&(x_1^2 + ax_2^2 + bx_3^2 + abx_4^2)(y_1^2 + ay_2^2 + by_3^2 + aby_4^2)\\ &= (x_1y_1 - ax_2y_2 - bx_3y_3 - abx_4y_4)^2 + a(x_1y_2 + x_2y_1 + bx_3y_4 - bx_4y_3)^2\\ &\quad + b(x_1y_3 + x_3y_1 + ax_4y_2 - ax_2y_4)^2 + ab(x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

If $c \in D_F(\langle\langle a, b\rangle\rangle)$ then $\dfrac{1}{c} = c\left(\dfrac{1}{c}\right)^2 \in D_F(\langle\langle a, b\rangle\rangle)$.

1.4. PROPOSITION. *Let* $a, b, c \in F^\times$. *If* $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ *is isotropic over* F *then* $\langle\langle b, c\rangle\rangle \perp \langle a\rangle$ *is isotropic over* F.

Proof. We can assume $\langle\langle b, c\rangle\rangle$ and hence $\langle 1, b, c\rangle$ is not isotropic over F otherwise we are done. By Lemma 1.2 (b), there exists $x_i \in F$ such that $-c = x_1^2 + ax_2^2 + bx_3^2 + abx_4^2$. Then $x_1^2 + bx_3^2 + c = -a(x_2^2 + bx_4^2)$ and both sides are nonzero since $\langle 1, b, c\rangle$ is not isotropic over F. It follows $-a = \dfrac{x_1^2 + bx_3^2 + c}{x_2^2 + bx_4^2} \in D_F(\langle\langle b, c\rangle\rangle)$ since $D_F(\langle\langle b, c\rangle\rangle)$ is a subgroup of $F^\times$ by Lemma 1.3. Therefore $\langle\langle b, c\rangle\rangle \perp \langle a\rangle$ is isotropic over F by Lemma 1.2 (b).

We see from Lemma 1.2 (b) that the Main Theorem is equivalent to the following more convenient formulation.

1.1′. THEOREM. *Let* $a, b, c \in \mathbf{Q}^\times$. *If* a, b, c *are not all positive, then* $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ *is isotropic over* $\mathbf{Q}$.

We begin now setting up the proof of the Main Theorem. We can assume $a, b, c \in \mathbf{Z}$ since a, b, c can be replaced by $a\alpha^2, b\beta^2, c\gamma^2$ for any nonzero $\alpha, \beta, \gamma \in \mathbf{Z}$. Suppose the Main Theorem is false. Then there exist nonzero $a, b, c \in \mathbf{Z}$, not all positive, such that $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is not isotropic over $\mathbf{Q}$. We can assume $|a| + |b| + |c|$ is minimal among all such counter-examples and we can assume $|a| \leqslant |b| \leqslant |c|$ by Proposition 1.4.

1.5. LEMMA. *Continue the assumptions from above. Then* $|b| < |c|$ *and* $|c|$ *is an odd prime number.*

Proof. If $|c| = 1$, then $|a| = |b| = 1$ and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ since a, b, c are not all positive. Thus $|c| > 1$.

Suppose $|b| = |c|$. If $c = -b$ then $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over Q, a contradiction. If $b = c$ then $\langle\langle a, b\rangle\rangle \perp \langle b\rangle$ is not isotropic over $\mathbf{Q}$. Then Proposition 1.4 implies $\langle\langle b, b\rangle\rangle \perp \langle a\rangle \cong \langle\langle 1, b\rangle\rangle \perp \langle a\rangle$ is not isotropic over $\mathbf{Q}$. But $1 + |b| + |a| < |a| + |b| + |c|$ and a, b are not both positive (since $b = c$). This contradicts the minimality assumption and therefore $|b| < |c|$.

Suppose $|c|$ is not a prime number and let $-c = (-c_1)(-c_2)$ where $|c_1|, |c_2| < |c|$. If $c < 0$, we can assume in addition that $c_1, c_2 < 0$. Then $\langle\langle a, b\rangle\rangle \perp \langle c_i\rangle$, $i = 1, 2$, both have at least one of a, b, c_i negative. Since $|a| + |b| + |c_i| < |a| + |b| + |c|$, it follows $\langle\langle a, b\rangle\rangle \perp \langle c_i\rangle$ is isotropic over $\mathbf{Q}$, $i = 1, 2$. Then $-c_1, -c_2 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ by Lemma 1.2 (b) and $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ by Lemma 1.3. This implies $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ by Lemma 1.2 (b), a contradiction. Therefore $|c|$ is a prime number.

If $|c| = 2$, then $|a| = |b| = 1$. If $a = -1$ or $b = -1$ then $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$. If $a = b = 1$, then $c = -2$ and $\langle\langle 1, 1\rangle\rangle \perp \langle -2\rangle$ is isotropic over $\mathbf{Q}$. These contradictions imply $|c| \neq 2$ and therefore $|c|$ is an odd prime.

To finish the proof of the Main Theorem we are reduced to proving Theorem 1.6:

1.6. THEOREM. *Suppose* p *is an odd prime,* $a, b \in \mathbf{Z}$, *and* $0 < |a|, |b| < p$. *Then there exists* $m \in \mathbf{Z}$, $0 < |m| < p$, *such that* $2mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

We shall assume Theorem 1.6 has been proved and finish the proof of the Main Theorem now. We apply Theorem 1.6 with $|c|$ in place of p. Then there exists $m \in \mathbf{Z}$, $0 < |m| < |c|$, such that $2m|c| \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. Our minimality assumption implies $\langle\langle a, b\rangle\rangle \perp \langle -|m|\rangle$ and $\langle\langle a, b\rangle\rangle \perp \langle -2\rangle$ are both isotropic over $\mathbf{Q}$. Then $2, |m|$ and hence $2|m|$ all lie in $D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. If $a, b > 0$ then $c < 0$ and it must be that $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. If either $a < 0$ or $b < 0$ then $-1 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ since $\langle\langle a, b\rangle\rangle \perp \langle 1\rangle$ is isotropic over $\mathbf{Q}$ by our minimality assumption. Therefore $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ in both cases and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$. This contradicts our assumption that a counterexample to the Main Theorem exists and finishes the proof of the Main Theorem.

Remark. A natural attempt to finish the proof of the Main Theorem would be a version of Theorem 1.6 where one finds $M \in \mathbf{Z}$, $0 < |M| < p$, such that $Mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. But according to [Mo], p. 169, one can only guarantee $|M| \leqslant \sqrt{2|ab|} < \sqrt{2p^2} = \sqrt{2}\,p$. If one could also make M even, then this result in [Mo] would give a proof of Theorem 1.6.

It remains to prove Theorem 1.6. If p is an odd prime, let $\left(\frac{c}{p}\right)$ be the Legendre symbol: If $(c, p) = 1$, then $\left(\frac{c}{p}\right) = \pm -1$ where $c^{\frac{p-1}{2}} \equiv \left(\frac{c}{p}\right) \bmod p$. In the course of proving Theorem 1.6 we will use the following result.

1.7. THEOREM. *Let p be an odd prime, $p \neq 5$, and let a, b be integers such that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Then there exist $x, y \in \mathbf{Z}$ such that $\left(\frac{ax^2 + by^2}{p}\right) = -1$ and $x^2 + y^2 < p$.*

We shall assume Theorem 1.7 has been proved and give now the

Proof of Theorem 1.6. If $\langle\langle a, b\rangle\rangle$ is isotropic over Q then we are done by Lemma 1.2(a). Now assume $\langle\langle a, b\rangle\rangle$ is not isotropic over Q. First assume at least one of $-a, -b, -ab$ is a quadratic residue mod p. Let $\alpha \in \{-a, -b, -ab\}$ where $\left(\frac{\alpha}{p}\right) = 1$. There exists β, $1 \leqslant \beta \leqslant p-1$, such that $p \mid \beta^2 - \alpha$ and $\beta^2 - \alpha$ is even (replace β by $p - \beta$ if necessary). Then $|\beta^2 - \alpha| \leqslant \beta^2 + |\alpha| < p^2 + p^2 = 2p^2$. Therefore, $\beta^2 - \alpha = 2mp$ where $0 < |m| < p$ and $2mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

If $p \equiv 1 \bmod 4$ then at least one of $-a, -b, -ab$ is a quadratic residue mod p since $\left(\frac{-1}{p}\right) = 1$ and $p \nmid ab$. Now suppose $p \equiv 3 \bmod 4$. Then at least one of $-a, -b, -ab$ is a quadratic residue mod p unless $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Suppose $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$ and choose x, y as in Theorem 1.7. Since $p \equiv 3 \bmod 4$, we have $-(ax^2+by^2)$ is a quadratic residue mod p and hence there exists β, $1 \leqslant \beta \leqslant p-1$, such that $p \mid \beta^2 + ax^2 + by^2$ and $\beta^2 + ax^2 + by^2$ is even. Then $|\beta^2 + ax^2 + by^2| \leqslant \beta^2 + |a|x^2 + |b|y^2 < p^2 + p(x^2+y^2) < 2p^2$. Therefore, $\beta^2 + ax^2 + by^2 = 2mp$ where $0 < |m| < p$ and $\beta^2 + ax^2 + by^2 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

The proof of Theorem 1.7 is given in the next section. Although we need Theorem 1.7 only when $p \equiv 3 \bmod 4$ we give a complete proof since very little additional work is required.

§ 2. The proof of Theorem 1.7

In this section p denotes an odd prime number. We begin by recalling a result about sequences of quadratic residues and nonresidues mod p.

2.1. Lemma. *The number of pairs* $(n, n+1)$ *in the set* $\{1, 2, ..., p-1\}$ *such that* $\left(\frac{n}{p}\right) = 1, \left(\frac{n+1}{p}\right) = -1$ *is equal to* $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$.

Proof. This elementary result is proved completely in [Ha], p. 157-158. (See also [An], Chapter 10.)

The next two lemmas give a way to count the number of lattice points $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, $x, y > 0$, satisfying the conditions of Theorem 1.7.

Let

$$\mathscr{S}(x) = \{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} \mid \alpha, \beta > 0, \alpha^2 + \beta^2 < x^2\}$$

and let $\mathscr{P}(x) = \{(\alpha, \beta) \in \mathscr{S}(x) \mid (\alpha, \beta) = 1\}$. Let $S(x) = |\mathscr{S}(x)|$ and $P(x) = |\mathscr{P}(x)|$. (It will be clear from context whether we mean the point (α, β) or the greatest common divisor of α, β.)

2.2. Lemma. *Let* R *be the set of nonzero squares* mod p.

(a) *The function* $\theta : \mathscr{P}(\sqrt{p}) \to R$ *given by* $\theta(x, y) = \dfrac{y^2}{x^2} \bmod p$ *is an injection.*

(b) $P(\sqrt{p}) \leqslant \frac{1}{2}(p-1)$.

Proof. Clearly (a) implies (b) since $|R| = \frac{1}{2}(p-1)$. If (a) is false then there exist two distinct points $(x_1, y_1), (x_2, y_2)$ in $\mathscr{P}(\sqrt{p})$ such that $\dfrac{y_1^2}{x_1^2} \equiv \dfrac{y_2^2}{x_2^2} \bmod p$. Then $y_1^2 x_2^2 - x_1^2 y_2^2 = (y_1 x_2 + x_1 y_2)(y_1 x_2 - x_1 y_2) \equiv 0 \bmod p$. We have $y_1 x_2 + x_1 y_2 \neq 0$ since $x_i, y_i > 0$ and $y_1 x_2 - x_1 y_2 \neq 0$ otherwise $\dfrac{y_1}{x_1} = \dfrac{y_2}{x_2}$ and