

BASIC QUADRATIC FORMS: SUPPLEMENTARY MATERIAL

LARRY J. GERSTEIN

Page 87. In the statement of Lemma 4.20, insert “regular” after “binary.”

Page 156. The last statement in Remark 7.15(iii) asserts “there is at most one isometry class of unimodular $k[x]$ -lattices on a given quadratic $k(x)$ -space.” This result deserves a proof, especially since it is tacitly assumed near the end of the proof of the Cassels–Pfister Theorem (on page 182). The statement is equivalent to this claim: Suppose $A = \langle \alpha_1, \dots, \alpha_n \rangle$ and $B = \langle \beta_1, \dots, \beta_n \rangle$, with $\alpha_i, \beta_i \in k^*$, and suppose further that $A \cong B$ over $k(x)$; then $A \cong B$ over k (and hence $A \cong B$ over $k[x]$).

Proof of the claim. From the hypothesis, there is a matrix $T = (t_{ij}) \in GL_n(k(x))$ such that ${}^tTAT = B$. Then $(\det T)^2 \cdot \det A = \det B$, and hence $\det T \in k^*$. It follows that if k is finite then $A \cong B$ over k , since the quadratic k -spaces having A and B as Gram matrices have the same discriminant.

Now suppose k is infinite. Let $d = d(x)$ be a least common denominator of the t_{ij} . So $T = \left(\frac{s_{ij}}{d}\right)$, with $d = d(x)$, $s_{ij} = s_{ij}(x) \in k[x]$. Then

$${}^t(s_{ij})A(s_{ij}) = {}^t(dT)A(dT) = \langle \beta_1 d^2, \dots, \beta_n d^2 \rangle.$$

Choose an element $\lambda \in k$ that is not a root of $d(x)$, and evaluate each polynomial in the preceding display at λ , obtaining

$${}^t(s_{ij}(\lambda))A(s_{ij}(\lambda)) = \left\langle \beta_1 (d(\lambda))^2, \dots, \beta_n (d(\lambda))^2 \right\rangle \cong B \quad \text{over } k,$$

proving the claim. □

Page 185. Theorem 9.14 reads as follows: *If $1 \leq n \leq 4$, then a positive integer is a sum of n integer squares if and only if it is a sum of n rational squares.* From this theorem the theorems of Lagrange, Fermat, and Gauss on sums of $n \leq 4$ squares are deduced in succession as corollaries. The proof of Theorem 9.14 in the book is based on the claim that the unimodular \mathbb{Z} -lattices $L \cong \langle 1, \dots, 1 \rangle$ of rank $n \leq 4$, which (by Hermite’s inequality on the minimum) have class number 1, are also \mathbb{Z} -maximal. The proof of \mathbb{Z} -maximality is correct for $n \leq 3$, but a reader has pointed out that the claim is false for $n = 4$: over the ring \mathbb{Z}_2 of 2-adic integers the lattice $L_2 = \mathbb{Z}_2 L$ is not \mathbb{Z}_2 -maximal, and hence L is not \mathbb{Z} -maximal. In fact if $\{e_1, \dots, e_4\}$ is an orthonormal basis for L , and $e'_1 = \frac{1}{2}(e_1 + e_2 + e_3 + e_4)$, then the

integral \mathbb{Z} -lattice $M = \mathbb{Z}e'_1 + \mathbb{Z}e_2 + \mathbb{Z}e_3 + \mathbb{Z}e_4$ (this is the **Hurwitz lattice**) is \mathbb{Z} -maximal. This follows from the fact that over \mathbb{Z}_2 there is the splitting

$$M_2 \cong \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \perp \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

in the basis $\{e'_1, e_2, e_3 - e_4, e_1 - e_4\}$. (In my maximality argument over \mathbb{Z}_2 , I overlooked this lattice.) Notice that $M \supset L$ and $(M : L) = 2$.

Here is a way to correct the error. In the proof of Theorem 9.14, retain the present proofs when $n = 2$ and $n = 3$, but if $n = 4$ defer the proof until after the corollaries. After the theorem (for $n = 2$ and 3), deduce Fermat's Two-Square Theorem and Gauss's Three-Square theorem (the present Corollaries 9.16 and 9.17). And then we have

Argument 1 for Lagrange's Theorem [Corollary 9.15]. By Gauss's Theorem it remains only to show that every positive integer of the form $n = 4^\nu(8k + 7)$, with $k \in \mathbb{Z}$, can be expressed as a sum of four integer squares. The equation

$$n - 4^\nu = 4^\nu(8k + 6) = x^2 + y^2 + z^2$$

is solvable with $x, y, z \in \mathbb{Z}$, and hence $n = (2^\nu)^2 + x^2 + y^2 + z^2$.

For another proof of Lagrange's Theorem, we first need a result that should have been in the book, namely

Theorem. *Let L be a \mathbb{Z} -lattice on the regular \mathbb{Q} -space V , and let K be a \mathbb{Z} -lattice in V . Suppose for each prime p there is a representation $K_p \rightarrow L_p$. Then there is a lattice $L' \in \text{gen } L$ such that $K \rightarrow L'$.*

Proof. By the invariant factor theorem we know that $K_p \subseteq L_p$ for almost all primes p , say for all p outside some finite set T . Each representation $\lambda_p : K_p \rightarrow L_p$ extends (via Witt) to an isometry $\hat{\lambda}_p \in O(V_p)$. So $\hat{\lambda}_p^{-1}L_p \supseteq K_p$. Now define the desired \mathbb{Z} -lattice L' by

$$L'_p = \begin{cases} \hat{\lambda}_p^{-1}L_p & \text{if } p \in T, \\ L_p & \text{if } p \notin T. \end{cases}$$

□

Corollary. If $h(L) = 1$ and $\alpha \rightarrow V$ and $\alpha \rightarrow L_p$ for all p , then $\alpha \rightarrow L$.

With the help of this corollary, we now give another proof of Lagrange's Theorem, and this proof will not rely on Gauss's Theorem.

Argument 2 for Lagrange's Theorem. Since $h(L) = 1$, it suffices to show that if $n \in \mathbb{N}$ then $n \rightarrow L_p$ for all primes p . Without loss of generality we can suppose that n is squarefree. For each prime $p \neq 2$ the localization L_p is \mathbb{Z}_p -maximal; and since the underlying

\mathbb{Q}_p -space is universal there is a representation $n \rightarrow L_p$. Now consider representations by L_2 . If n is odd then $n \equiv 1, 3, 5, 7 \pmod{8}$. But each of $1, 3, 5, 7$ is obviously represented by L_2 , hence so is n , by the Local Square Theorem. If n is even then $n \equiv 2m \pmod{16}$, with $m \in \{1, 3, 5, 7\}$, and therefore $n = 2m\varepsilon^2$ for some $\varepsilon \in \mathbb{Z}_2^*$. Since each of the values $2m$ is represented by L_2 , we are done. \square

With Lagrange's Theorem in hand, the proof of Theorem 9.14 is now complete.

Page 189. In the statement of Theorem 9.19, the inequalities $r, s \geq 1$ should replace the inequalities $r, s \geq 0$. Also, towards the end of the proof of Theorem 9.19 is the instruction "apply the induction hypothesis to the orthogonal complement of M ." More accurately, the induction hypothesis should be applied to the orthogonal complement of $\mathbb{Z}v_1$ or $\mathbb{Z}v_2$, at least one of which is guaranteed to be indefinite.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SANTA BARBARA, CA 93106.
E-mail address: gerstein@math.ucsb.edu