Remarks on the Stufe of Fields

By Genjiro FUJISAKI

Department of Mathematics, College of General Education, University of Tokyo, Komaba, Meguro-ku, Tokyo

(Received January 31, 1973)

1. Let A be a commutative ring with an identity 1. The "*Stufe*" of A is the smallest number of squares possible in such a representation that $-1=a_1^2+\cdots+a_s^2$, $a_i\in A$ $(i=1, \cdots, s)$, and is denoted by $s(A)$. If such a representation is impossible, $s(A)=\infty$. A. Pfister [6] has shown that, for arbitrary field F of characteristic not 2, $s(F)$ is a power of 2 or ∞. M. Knebusch [4] has shown, in generalizing Pfister's theorem, that $s(A)$ of a local ring A is a power of 2 or ∞ if 2 is a unit in A; if 2 is not a unit, $s(A)$ is a power of 2 or ∞ or a number of form 2^n-1.

Now, let F be a field with an additive valuation, and O be the valuation ring in F. Then O is a local ring with its quotient field F. In this case, we shall prove the following proposition.

Proposition. *Let F be a field with an additive valuation and O be the valuation ring in F. Then we have $s(O)=s(F)$.*

*Proof.** It suffices to prove $s(O)\leqq s(F)=s$. Let $-1=e_1^2+\cdots+e_s^2$, $e_i\in F$. If all $e_i\in O$, then done. Suppose $W(e_1)=\min_{1\leq i\leq s}\{W(e_i)\}<0$, where W denotes the valuation of F. Then $-1=(e_1^{-1})^2+\left(\frac{e_2}{e_1}\right)^2+\cdots+\left(\frac{e_s}{e_1}\right)^2$, e_1^{-1}, $\frac{e_i}{e_1}\in O$ $(i=2, \cdots, s)$, whence $s(O)\leqq s=s(F)$.

2. Let $F_\mathfrak{p}$ be a finite extention of rational p-adic number field Q_p and $O_\mathfrak{p}$ be its ring of integers. The quadratic form $\sum_{i=1}^{5} X_i^2$ has, by a well known theorem, a non-trivial zero in $F_\mathfrak{p}$, whence $s(F_\mathfrak{p})\leqq 4$. If $\mathfrak{p}\nmid 2$, i.e., $F_\mathfrak{p}$ is an extension of Q_p, $p\neq 2$, then $-1\equiv x^2+y^2 \mod \mathfrak{p}$ has always a solution in $O_\mathfrak{p}$. Hence, by Hensel's lemma, $-1=x^2+y^2$ has a solution in $O_\mathfrak{p}$, whence $s(F_\mathfrak{p})\leqq 2$. Note that if $\mathfrak{p}\nmid 2$, $s(F_\mathfrak{p})=1 \Leftrightarrow \sqrt{-1}\in F_\mathfrak{p} \Leftrightarrow N\mathfrak{p}\equiv 1 \pmod 4$ and $s(F_\mathfrak{p})=2 \Leftrightarrow N\mathfrak{p}\equiv 3 \pmod 4$.

Now let $\mathfrak{p}|2$, i.e., $F_\mathfrak{p}$ be an extension of 2-adic number field Q_2. We may suppose $\sqrt{-1}\notin F_\mathfrak{p}$. Then "$-1=x^2+y^2$ has a solution in $F_\mathfrak{p}$" $\Leftrightarrow$ "$-1\in N_{F_\mathfrak{p}(\sqrt{-1})/F_\mathfrak{p}}(F_\mathfrak{p}(\sqrt{-1}))$" $\Leftrightarrow$ "cyclic algebra $A_\mathfrak{p}=(-1, F_\mathfrak{p}, \sigma)$ splits", where σ denotes a generating automorphism of $F_\mathfrak{p}(\sqrt{-1})$ over $F_\mathfrak{p}$. But the cyclic algebra

* Author owes this proof to Prof. Y. Watanabe, to whom he is thankful.

$A_{\mathfrak{p}}$ is nothing but the quaternion algebra over $F_{\mathfrak{p}}$, $F_{\mathfrak{p}}+F_{\mathfrak{p}}i+F_{\mathfrak{p}}j+F_{\mathfrak{p}}k$, with $i^2=j^2=-1$, $k=ij=-ji$.

Denoting by D_2 the quaternion algebra over Q_2, $Q_2+Q_2i+Q_2j+Q_2k$, with $i^2=j^2=-1$, $k=ij=-ji$, we have $A_{\mathfrak{p}}=D_2\otimes_{Q_2}F_{\mathfrak{p}}$, and the invariant $inv_{\mathfrak{p}} A_{\mathfrak{p}}\equiv[F_{\mathfrak{p}}: Q_2]\, inv_2(D_2) (mod\, 1)$. As it is well known that $inv_2(D_2)=\frac{1}{2}$. $A_{\mathfrak{p}}$ splits if and only if $[F_{\mathfrak{p}}: Q_2]\equiv 0$ $(mod\, 2)$. Hence we have the following proposition. (cf. [1])

Proposition. *Let $F_{\mathfrak{p}}$ be a finite extension of p-adic field Q_p. If $\mathfrak{p}\nmid 2$ then $s(F_{\mathfrak{p}})\leqq 2$. If $\mathfrak{p}|2$ and $\sqrt{-1}\notin F$, then $s(F_{\mathfrak{p}})=2$ if and only if $[F_{\mathfrak{p}}: Q_2]\equiv 0$ $(mod\, 2)$, and $s(F)=4$ otherwise.*

Corollary. (cf. [1] p. 21). *Denoting by $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$ the quadratic norm residue symbol in $F_{\mathfrak{p}}$, we have*

$$\left(\frac{-1,\ -1}{\mathfrak{p}}\right)=\begin{cases} 1 & \text{for } \mathfrak{p}\nmid 2 \\ (-1)^{[F_{\mathfrak{p}}:\, Q_2]} & \text{for } \mathfrak{p}|2. \end{cases}$$

Proof. $\left(\frac{-1,\ -1}{\mathfrak{p}}\right)$ is 1 if and only if $1=-x^2-y^2$ has a solution in $F_{\mathfrak{p}}$ and -1 otherwise.

3. Let F be an algebraic number field of finite degree. The Stufe $s(F)=\infty$ if and only if F has a real conjugate, whence $s(F)<\infty$ implies that F is a totally imaginary number field. Suppose $s(F)<\infty$. Then the Hasse principle shows that the quadratic form $\sum_{i=1}^{5} X_i^2$ has a non-trivial zero in F, whence $s(F)\leqq 4$. Hence $s(F)=1, 2, 4$ or ∞. But $s(F)=1$ means simply $\sqrt{-1}\in F$. We shall give another proof of the following well known theorem ([1], [2], [3]). Our proof is essentially the same as one in [2].

Theorem. *Let F be an algebraic number field of finite degree. Then $s(F)\leqq 2$ if and only if F is totally imaginary and the local degrees of F at all primes of F extending the rational prime 2 are even.*

Proof. We may suppose $\sqrt{-1}\notin F$. Then, "$-1=x^2+y^2$ has a solution in F" if and only if $-1\in N_{F(\sqrt{-1})/F}(F(\sqrt{-1}))$, which is equivalent to the statement: "the cyclic algebra $A=(-1, F(\sqrt{-1})/F, \sigma)$ splits, where σ is a generating automorphism of $F(\sqrt{-1})/F$." A splits over F if and only if A splits locally everywhere. But A is nothing but the ordinary quaternion algebra $F+Fi+Fj+Fk$, $i^2=j^2=-1$, $ij=k=-ji$, whence $A=D\otimes_Q F$, where D is the ordinary quaternion algebra over Q, and the $\mathfrak{p}$-invariant $inv_{\mathfrak{p}} A=[F_{\mathfrak{p}}: Q_p]\, inv_p D$ for $\mathfrak{p}|p$. Since D has invariant $\frac{1}{2}$ at prime divisor 2, $\frac{1}{2}$ at ∞, and 0 at all other prime divisors of Q, A splits, therefore, if and only if $F_{\mathfrak{p}}=C$ (the complex field) for all infinite primes $\mathfrak{p}$ and $[F_{\mathfrak{p}}: Q_2]\equiv 0\ (mod\ 2)$ for all $\mathfrak{p}|2$. This proves the Theorem.

4. Finally we shall make a simple remark on the Stufe of fields.

Proposition. *Let F be a field of characteristic not 2 and $\sqrt{-1}\notin F$. Then $s(F)=2$ if and only if there exists such a cyclic extension E over F that $[E: F]=4$ and $E\supset F(\sqrt{-1})$.*

Hence, for a finite algebraic number field F, not containing $\sqrt{-1}$, there exists a cyclic extension E over F, of degree 4 and $E\supset F(\sqrt{-1})$, if and only if F is totally imaginary and the local degrees of F at all primes extending the rational prime 2 are even.

This proposition follows, for example, from N. Bourbaki, Algebre, Chap. V §11 Exercices 7).

References

[1] Connell, I. G., The Stufe of Number Fields, *Math. Z.*, **124**, 20-22 (1972).
[2] Fein, B., Gordon, B., and Smith, J., On the Representation of −1 as a Sum of Two Squares in an Algebraic Number Fields, *J. Number Theory* **3**, 310-315 (1971).
[3] Hasse, H., Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, *J. reine u. angew. Math.*, **152**, 113-130 (1924).
[4] Knebusch, M., Runde Formen über semi-localen Ringen, *Math. Ann.*, **193**, 21-34 (1971).
[5] Peters, M., Die Stufe von Ordnungen ganzer Zahlen in algebraischen Zahlkörpern, *Math. Ann.*, **195**, 309-314 (1972).
[6] Pfister, A., Zur Darstellung von −1 als Summe von Quadraten in einem Körper, *J. London Math. Soc.*, **40**, 159-165 (1965).