QUADRATIC FIELDS IN WHICH FACTORIZATION IS ALWAYS UNIQUE*

BY L. E. DICKSON

1. *Definitions.* Let m be an integer, other than 0 and 1, such that m is not divisible by a perfect square exceeding unity. All numbers $r+s\sqrt{m}$ in which r and s are rational constitute a *field* $R(\sqrt{m})$. Its *algebraic integers* are known to be $x+y\theta$, where x and y are rational integers, and

(1) $\theta=\sqrt{m}$ if $m\equiv 2$ or $m\equiv 3 \pmod 4$,

(2) $\theta=\frac{1}{2}(1+\sqrt{m}),\ \theta^2=\theta-k,$ if $m\equiv 1 \pmod 4$,

where $k=\frac{1}{4}(1-m)$. The *conjugate* of $\xi=x+y\theta$ is defined to be $\xi'=x+y\theta'$, where $\theta'=-\theta$ in case (1), and $\theta'=\frac{1}{2}(1-\sqrt{m})$ in case (2). The product $\xi\xi'$ is called the *norm* of ξ, and is denoted by $N(\xi)$. According as the case is (1) or (2), we have

(3) $N(x+y\theta)=x^2-my^2$ or $x^2+xy+ky^2$.

If ξ is an algebraic integer such that $N(\xi)=\pm 1$, then ξ is called a *unit.* The only units in $R(i)$ are ± 1 and $\pm i$.

2. *Object of the Paper.* It is known† that $-1, -2, -3, -7$ and -11 are the only negative values of m for which the greatest common divisor process yielding numerically decreasing norms is always applicable in $R(\sqrt{m})$, so that if a and b are any algebraic integers ($b\neq 0$) there exist algebraic integers q and r of the field such that

$$a=bq+r,\quad |\text{norm } r|<|\text{norm } b|.$$

---

* Presented to the Society, December 29, 1923. See also This Bulletin, p. 90, Jan.–Feb., 1924, and footnote, p. 247, May–June, 1924.

† For a geometric proof, see Birkhoff, American Mathematical Monthly, vol. 13 (1906), pp. 156–159.