118. *A Remark on the Arithmetic in a Subfield.*

By Keizo ASANO and Tadasi NAKAYAMA.
Mathematical Institute, Osaka Imperial University.

(Comm. by T. TAKAGI, M.I.A., Dec. 12, 1940.)

Let K be a (commutative) field and k be its subfield over which K has a finite degree. It is well known that if k is a quotient field of a certain integrity-domain in which the usual arithmetic[1] holds then the same is the case in the integrity-domain in K consisting of the totality of relatively integral elements. The present small remark is however concerned with the converse situation. Suppose namely *K be a quotient field of an integrally closed integrity-domain $\mathfrak{O}$.* Does then the integrity-domain

$$\mathfrak{o}=\mathfrak{O}\cap k$$

in k have the usual arithmetic if we have it in $\mathfrak{O}$? The answer is of course negative in general.[2] So we want to obtain a condition that the usual arithmetic prevail in $\mathfrak{o}$. And, to do so we can, and shall, assume without any essential loss in generality that *K/k be normal,* since we know that the usual arithmetic is preserved by any finite extension.

Theorem 1. In order that $\mathfrak{o}=\mathfrak{O}\cap k$ possess the usual arithmetic it is necessary and sufficient that the intersection $\mathfrak{O}^*=\mathfrak{O}\cap\mathfrak{O}'\cap\dots\cap\mathfrak{O}^{(n-1)}$ $\big(n=(K:k)\big)$ of all the conjugates (with respect to K/k) of $\mathfrak{O}$ in K have it. And, if this is the case then $\mathfrak{O}^*$ is the totality of the elements in K relatively integral with respect to $\mathfrak{o}$.

Theorem 2. If in particular $\mathfrak{O}$ coincides with all its conjugates and if we have the usual arithmetic in $\mathfrak{O}$ then we have it in $\mathfrak{o}$ too.

We begin with a proof of this special case: First, k is the quotient field of $\mathfrak{o}$. For, if $a\in k$ then $a\alpha\in\mathfrak{O}$ for a suitable $\alpha\in\mathfrak{O}$ and so $aN(\alpha)\in\mathfrak{o}$, where $N(\alpha)$ is the norm $\alpha\alpha'\dots\alpha^{(n-1)}$ of α and lies in $\mathfrak{o}=\mathfrak{O}\cap k$ since $\alpha,\alpha',\dots$ are all in $\mathfrak{O}$.

Let $\mathfrak{a}$ be an (integral or fractional) $\mathfrak{o}$-ideal in k. $\mathfrak{a}\mathfrak{O}$ has the inverse $(\mathfrak{a}\mathfrak{O})^{-1}$ and $\mathfrak{a}(\mathfrak{a}\mathfrak{O})^{-1}=(\mathfrak{a}\mathfrak{O})(\mathfrak{a}\mathfrak{O})^{-1}=\mathfrak{O}$. Hence

$$1=a_1\alpha_1+a_2\alpha_2+\dots+a_r\alpha_r \quad\text{with}\quad a_\mu\in\mathfrak{a},\quad \alpha_\mu\in(\mathfrak{a}\mathfrak{O})^{-1},$$

and

$$1=\prod_{i=0}^{n-1}(a_1\alpha_1^{(i)}+\dots+a_r\alpha_r^{(i)})=\sum c_{\nu_1\dots\nu_r}a_1^{\nu_1}\dots a_r^{\nu_r},$$

where $c_{\nu_1\dots\nu_r}$ are homogeneous of degree n in $\alpha_1,\dots,\alpha_r,\alpha_1',\dots,\alpha_r',\dots$. Now, let $\mathfrak{P}$ be a prime ideal in $\mathfrak{O}$, and let $\mathfrak{O}_\mathfrak{P}$ be the ring of integers for $\mathfrak{P}$, that is, the valuation ring for $\mathfrak{P}$. Then $\mathfrak{o}_\mathfrak{P}=\mathfrak{O}_\mathfrak{P}\cap k$ is the valuation ring of the valuation in k induced by $\mathfrak{P}$. We set $\mathfrak{a}_\mathfrak{P}=\mathfrak{a}\mathfrak{o}_\mathfrak{P}$,

1) Unique factorization into prime ideals = Group condition.
2) See an example below.