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 $\mathfrak{O}^*=\mathfrak{O}\cap\mathfrak{O}'\cap\dots\cap\mathfrak{O}^{(n-1)}$ $(n=(K:k))$ 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.

$\mathfrak{O}_1 = \mathfrak{O}\mathfrak{o}_{\mathfrak{P}}$. Then $\mathfrak{O}_1 \leqq \mathfrak{O}_{\mathfrak{P}}$ and $\mathfrak{O}_1 \frown k = \mathfrak{O}_{\mathfrak{P}} \frown k = \mathfrak{o}_{\mathfrak{P}}$. The inverse $\mathfrak{a}_{\mathfrak{P}}^{-1}$ of $\mathfrak{a}_{\mathfrak{P}}$ with respect to $\mathfrak{o}_{\mathfrak{P}}$ exists; $\mathfrak{a}_{\mathfrak{P}}^{-1}\mathfrak{a}_{\mathfrak{P}} = \mathfrak{o}_{\mathfrak{P}}$. Further

$$(\mathfrak{a}\mathfrak{O})^{-1}\mathfrak{o}_{\mathfrak{P}} = (\mathfrak{a}\mathfrak{O})^{-1}\mathfrak{a}_{\mathfrak{P}}\mathfrak{a}_{\mathfrak{P}}^{-1} = \mathfrak{O}\mathfrak{o}_{\mathfrak{P}}\mathfrak{a}_{\mathfrak{P}}^{-1} = \mathfrak{a}_{\mathfrak{P}}^{-1}\mathfrak{O}_1$$

and so

$$\alpha_\mu \in (\mathfrak{a}\mathfrak{O})^{-1} \leqq \mathfrak{a}_{\mathfrak{P}}^{-1}\mathfrak{O}_1, \qquad \alpha_\mu^{(i)} \in \mathfrak{a}_{\mathfrak{P}}^{-1}\mathfrak{O}_1.$$

Therefore

$$c_{\nu_1\ldots\nu_r} \in (\mathfrak{a}_{\mathfrak{P}}^{-1}\mathfrak{O}_1)^n = \mathfrak{a}_{\mathfrak{P}}^{-n}\mathfrak{O}_1 \quad \text{whence} \quad \in \mathfrak{a}_{\mathfrak{P}}^{-n}\mathfrak{O}_1 \frown k = \mathfrak{a}_{\mathfrak{P}}^{-n}.$$

Since this is the case for every $\mathfrak{P}$, we have $c_{\nu_1\ldots\nu_r} \in \frown \mathfrak{a}_{\mathfrak{P}}^{-n}$, and thus $1 \in (\frown \mathfrak{a}_{\mathfrak{P}}^{-n})\mathfrak{a}^n$. But $\mathfrak{a}_{\mathfrak{P}}^{-n}\mathfrak{a}^n \leqq \mathfrak{o}_{\mathfrak{P}}$ and $(\frown \mathfrak{a}_{\mathfrak{P}}^{-n})\mathfrak{a}^n \leqq \mathfrak{o}_{\mathfrak{P}} = \mathfrak{o}$. So $(\frown \mathfrak{a}_{\mathfrak{P}}^{-n})\mathfrak{a}^n = \mathfrak{o}$ and $\mathfrak{a}$ has an inverse. This proves our theorem 2.

A second proof: That an integrity-domain $\mathfrak{O}$ in K has K as its quotient field and possesses the usual arithmetic is equivalent to the existence of a system $\{\Phi_\sigma\}$ of non-archimedian valuations Φ_σ in K satisfying the condition:[1)]

1) $\mathfrak{O}$ is the intersection $\frown \mathfrak{O}_\sigma$ of valuation rings $\mathfrak{O}_\sigma$ for Φ_σ,

2) every Φ_σ is discrete,

3) given a finite number of indices, say $\sigma_1, \sigma_2, \ldots, \sigma_m$, and given correspondingly $a_1, a_2, \ldots, a_m \in K$, there exists an element a in K which is, for every $i = 1, 2, \ldots, m$, near to a_i with respect to Φ_{σ_i} to any preassigned degree and which is integral for all other Φ_σ.

Further, in case such a system exists any non-archimedian valuation in K whose valuation ring contains $\mathfrak{O}$ is equivalent to one (and only one) of Φ_σ.

Now, let k be, as before, a subfield of K over which K is finite and normal. On supposing the existence of $\{\Phi_\sigma\}$ in K as above, we want to derive a system of valuations in k satisfying the similar conditions. For this, we simply consider those valuations induced in k by Φ_σ and take representatives of the classes of mutually equivalent ones among them. Denote the system thus obtained by $\{\varphi_\tau\}$. It is evident that $\mathfrak{o} = \mathfrak{O} \frown k$ coincides with the intersection $\frown \mathfrak{o}_\tau$ of the valuation rings $\mathfrak{o}_\tau$ for φ_τ. Further, every φ_τ is discrete. To verify the third condition, we first assume K/k to be *separable*. Then every a in k is a trace of an element α in K; $a = S(\alpha) = \alpha + \alpha' + \cdots + \alpha^{(n-1)}$. Now, suppose φ_τ is induced by Φ_σ. A valuation conjugate to Φ_σ with respect to K/k is equivalent to a certain Φ, since $\mathfrak{O}$ coincides with its conjugates. Moreover, the Φ's conjugate to Φ_σ (up to equivalence) and only those divide φ_τ. So if an element β is close, sufficiently, to α at all those conjugate valuations then $S(\beta) = \beta + \beta' + \cdots + \beta^{(n-1)}$ is near to a with respect to φ_τ. When $\varphi_{\tau_1}, \varphi_{\tau_2}, \ldots, \varphi_{\tau_m}$ and $a_1, a_2, \ldots, a_m$ are given, where $a_i = S(\alpha_i)$, we let α_i be simultaneously approximated by β at the Φ's dividing φ_{τ_i}. The β can be chosen to be integral for all other Φ's. But then $b = S(\beta)$ has the desired property. Let next K/k be *purely inseparable*. Denote by p the characteristic of k, and let $K^q \leqq k$ where q is a power of p. Given $a_1, a_2, \ldots, a_m$, we consider the field

1) This formulation is due to E. Artin. In this connection cf. also M. Moriya, Journal of Hokkaido Imperial University (1940).

$$K_1 = K(\sqrt[q]{a_1},\ \sqrt[q]{a_2}, \cdots,\ \sqrt[q]{a_m}) \geqq K.$$

Since K_1/K is finite we have the usual arithmetic in K_1 and the corresponding system of valuation consists of the extensions of Φ's. Hence we can choose an element α in K_1 which is close to $\sqrt[q]{a_1}, \sqrt[q]{a_2}, \cdots, \sqrt[q]{a_m}$ at the extensions of $\varphi_{\tau_1}, \varphi_{\tau_2}, \cdots, \varphi_{\tau_m}$ and which is integral at all other valuations. Then $\alpha^q (\in k)$ approximates a_i at φ_{τ_i} and is integral at other places. Finally, a *general* case can readily be reduced to these extreme cases.

Proof of Theorem 1. It is now easy to deduce Theorem 1. We first observe that

$$\mathfrak{o} = \mathfrak{O} \frown k = \mathfrak{O}' \frown k = \mathfrak{O}'' \frown k \cdots \quad \text{whence} \quad \mathfrak{o} = \mathfrak{O}^* \frown k.$$

Hence if $\mathfrak{O}^*$ has the usual arithmetic then so does $\mathfrak{o}$ according to Theorem 2. Suppose conversely that $\mathfrak{o}$ possesses the usual arithmetic. Then it satisfies in particular the maximum condition, and therefore, an element in K integral with respect to $\mathfrak{o}$ is also integral with respect to $\mathfrak{O}$ and thus lies in $\mathfrak{O}$. Similarly the same element is contained in all the conjugates $\mathfrak{O}^{(i)}$ of $\mathfrak{O}$, and so it is in $\mathfrak{O}^*$. But conversely every element in $\mathfrak{O}^*$ is integral with respect to $\mathfrak{o}$, because all its conjugates are in $\mathfrak{O}^*$ and the coefficients of the (normalized) irreducible equation in k satisfied by it are all in $\mathfrak{o} = \mathfrak{O}^* \frown k$. So $\mathfrak{O}^*$ consists of the totality of the elements integral with respect to $\mathfrak{o}$, and therefore, it has the usual arithmetic along with $\mathfrak{o}$.

The additional remark in the theorem was proved at the same time.

Example that the usual arithmetic prevails in $\mathfrak{O}$ but not in $\mathfrak{o}$: Let Ω be a field whose characteristic is different from 2, and x, y be two independent variables. Put

$$k = \Omega(x, y), \quad K = k(\sqrt{x}) = \Omega(\sqrt{x}, y), \quad \mathfrak{O} = \Omega(\sqrt{x}+y)[y],$$

where crotchets mean ring-adjunction. Then $\mathfrak{o} = \mathfrak{O} \frown k = \Omega[x, y]$. For, if $\alpha \in \mathfrak{o}$ then

$$\alpha = F(x, y)/G(x, y) = f(\sqrt{x}, y)/g(\sqrt{x}+y),$$

where $F(x, y), G(x, y) \in \Omega[x, y], f(\sqrt{x}, y) \in \Omega[\sqrt{x}, y], g(\sqrt{x}+y) \in \Omega[\sqrt{x}+y]$ and where F and G are without common factor in $\Omega[x, y]$ and so are f and g in $\Omega[\sqrt{x}, y]$. But then F and G have no common factor in $\Omega[\sqrt{x}, y]$ either. Thus necessarily $F=f$, $G=g$ and therefore $G=g$ is simply a constant in Ω. So $\alpha \in \Omega[x, y]$.

Now clearly the usual arithmetic fails to prevail in $\mathfrak{o}$.

It is also easy to deduce the assertion from our general criterion in Theorem 1. Namely, an argument similar to the above one shows that $\mathfrak{O}^* = \mathfrak{O} \frown \mathfrak{O}' = \Omega[\sqrt{x}, y]$; $\mathfrak{O}' = \Omega(-\sqrt{x}+y)[y]$ being the conjugate of $\mathfrak{O}$.