Uchida, K.
Osaka J. Math.
14 (1977), 155–157

WHEN IS $Z[\alpha]$ THE RING OF THE INTEGERS?

Dedicated to the memory of Professor Taira Honda

Kôji UCHIDA

(Received December 15, 1975)

Let Z be the ring of the rational integers and let Q be the field of the rational numbers. Let α be an algebraic integer. Then $Z[\alpha]$ is a subring of the ring of the integers in $Q(\alpha)$. We will show when $Z[\alpha]$ is just the ring of the integers. We deal with this problem in slightly more general situation.

Let R be a Dedekind ring. A polynomial $f(X)$ of the form

$$f(X)=X^m+a_1X^{m-1}+\cdots+a_m\,,\ a_i\in R$$

is called an integral polynomial over R. Let S be an integral domain containing R. A element α of S is called integral over R if it is a zero of some integral polynomial over R. Then α is a zero of the integral irreduicble polynomial $\varphi(X)$ which is called the defining polynomial of α.

Theorem. *Let R be a Dedekind ring. Let α be an element of some integral domain which contains R, and let α be integral over R. Then $R[\alpha]$ is a Dedekind ring if and only if the defining polynomial $\varphi(X)$ of α is not contained in $\mathfrak{m}^2$ for any maximal ideal $\mathfrak{m}$ of the polynomial ring $R[X]$.*

First we prove the following lemma.

Lamma. *Let $\mathfrak{m}$ be a maximal ideal of $R[X]$. If $\mathfrak{m}$ contains an integral polynomial, $\mathfrak{m}$ is of the form $\mathfrak{m}=(\mathfrak{p}, f(X))$, where $\mathfrak{p}$ is a maximal iedal of R and $f(X)$ is an integral polynomial which is irreducible mod $\mathfrak{p}$.*

Proof. Let $g(X)$ be an integral polynomial in $\mathfrak{m}$. Then the residue class ring $R[X]/(g(X))$ is integral over R. Hence its maximal ideal contains a maximal ideal $\mathfrak{p}$ of R[1, Chap. V, 2]. Then $\mathfrak{m}$ also contains $\mathfrak{p}$. As any maximal ideal of $(R/\mathfrak{p})[X]$ is generated by an irreducible polynomial, $\mathfrak{m}$ is of the form $(\mathfrak{p}, f(X))$.

Remark. This lemma holds for any commutative ring with identity. If we drop out the condition that $\mathfrak{m}$ contains an integral polynomial, $\mathfrak{m}$ is not necessarily of the above form. For example, let R be a semilocal Dedekind ring and let a be in the intersection of all maximal ideals. Then $\mathfrak{m}=(aX-1)$ is a maximal ideal, because $R[X]/\mathfrak{m} \cong R[1/a]$ is a field. If a Dedekind ring R contains infinite number of maximal ideals, it can be shown that any maximal ideal is of the above form.

We now prove our theorem. Le $\varphi(X) \in \mathfrak{m}^2$ for some $\mathfrak{m}$.
As $\mathfrak{m}=(\mathfrak{p}, f(X))$ by the above lemma, it holds

$$a\varphi(X) = p^2 r(X) + pf(X)s(X) + f(X)^2 t(X),$$

where $p \in \mathfrak{p}$ such that $(p)=\mathfrak{p}\mathfrak{a}$, $(\mathfrak{p}, \mathfrak{a})=1$ and $a \in \mathfrak{a}^2 - \mathfrak{a}^2\mathfrak{p}$, $r(X)$, $s(X)$ and $t(X) \in R[X]$. We can assume deg $\varphi(X) = \deg f(X)^2 t(X)$.
Then

$$(f(\alpha)t(\alpha)/p)^2 + (f(\alpha)t(\alpha)/p)^2 s(\alpha) + r(\alpha)t(\alpha) = 0,$$

i.e., $f(\alpha)t(\alpha)/p$ is integral over $R[\alpha]$. As every element of $R[\alpha]$ is uniquely written as a polynomial of α of degree at most deg $\varphi(X)-1$ with coefficients in R, $f(\alpha)t(\alpha)/p$ is not an element of $R[\alpha]$ because $f(X)t(X) \not\equiv 0 \pmod{\mathfrak{p}}$. Hence $R[\alpha]$ is not integrally closed. Now let $\varphi(X) \notin \mathfrak{m}^2$ for any $\mathfrak{m}$. As $R[\alpha]$ is integral over R, every non-zero prime ideal is maximal. Then every non-zero ideal of $R[\alpha]$ contains a product of maximal ideals because $R[\alpha]$ is noetherian. If every maximal ideal is invertible, every non-zero ideal is equal to a product of maximal ideals and $R[\alpha]$ is a Dedekind ring. Let $\mathfrak{n}$ be any maximal ideal of $R[\alpha]$. Let $\mathfrak{m}$ be the inverse image of $\mathfrak{n}$ by the natural homomorphism $R[X] \to R[\alpha]$. Then $\mathfrak{m}=(\mathfrak{p}, f(X))$ because $\mathfrak{m}$ is maximal and $\varphi(X) \in \mathfrak{m}$. We can put

$$a\varphi(X) = ph(X) + af(X)k(X),$$

where p is an element of $\mathfrak{p}$ such that $(p)=\mathfrak{p}\mathfrak{a}$, $(\mathfrak{p}, \mathfrak{a})=1$, $a \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}$, $h(X)$ and $k(X) \in R[X]$. If $f(\alpha)=0$, $\mathfrak{n}=\mathfrak{p}R[\alpha]$ which is invertible. We now assume $f(\alpha) \neq 0$. As $a\varphi(X) \notin \mathfrak{m}^2$, it holds $h(X) \notin \mathfrak{m}$ or $ak(X) \notin \mathfrak{m}$, i.e., $h(\alpha) \notin \mathfrak{n}$ or $ak(\alpha) \notin \mathfrak{n}$. As aq/p is in R for every element q of $\mathfrak{p}$, the above equation shows that $ak(\alpha)/p$ is in $\mathfrak{n}^{-1}$. Then $h(\alpha) = -f(\alpha) \cdot ak(\alpha)/p$ and $ak(\alpha) = p \cdot ak(\alpha)/p$ are in $\mathfrak{n} \cdot \mathfrak{n}^{-1}$. As $h(\alpha)$ or $ak(\alpha)$ is not an element of $\mathfrak{n}$, it holds $\mathfrak{n} \cdot \mathfrak{n}^{-1} \not\subset \mathfrak{n}$. This shows $\mathfrak{n} \cdot \mathfrak{n}^{-1} = R[\alpha]$, i.e., $\mathfrak{n}$ is invertible. This completes the proof.

In the case $R=Z$, finite amount of calculations show if $\varphi(X)$ is contained in some $\mathfrak{m}^2$ or not. If $\varphi(X) \in \mathfrak{m}^2$ for $\mathfrak{m}=(p, f(X))$, it holds

$$\varphi(X) = p^2 r(X) + pf(X)s(X) + f(X)^2 t(X)$$

for some $r(X)$, $s(X)$ and $t(X) \in Z[X]$. This shows that $\varphi(X) \equiv 0 \pmod{p}$ has multiple roots, i.e., p is a prime factor of the discriminant of $\varphi(X)$. That is, only a finite number of prime numbers are possible. If such prime p is fixed, $f(X)$ must be a multiple factor of $\varphi(X)$ mod p.

EXAMPLE. Let $F_n(X)$ be the defining polynomial of a primitive n-th root ζ

of unity. It is known that $Z[\zeta]$ is the ring of the integers in $Q(\zeta)$. But the proof is not easy. We can show this more easily by our method. If $n=p^e$ is a power of a prime, this is very easy. But in the general case we must assume some arithmetic in $Q(\zeta)$. We only need to consider maximal ideals $\mathfrak{m}$ which contain prime factors of n. Let p be a prime factor fo n, and let $n=p^e m$, $(p, m)=1$. As $F_n(X)$ divides $F_m(X^{p^e})$ and as $F_m(X^{p^e}) \equiv F_m(X)^{p^e}$ (mod p), we can assume $\mathfrak{m}=(p, f(X))$, where $f(X)$ is an irreducible factor of $F_m(X)$ mod p. Let η be a primitive m-th root of unity. Then there exists a prime divisor $\mathfrak{p}$ of p in $Q(\eta)$ such that $f(\eta) \in \mathfrak{p}$. As $F_n(X)$ divides $F_{p^e}(X^m)$, it is enough to show that $F_{p^e}(X^m) \notin \mathfrak{m}^2$. If $F_{p^e}(X^m) \in \mathfrak{m}^2$, we can put

$$F_{p^e}(X^m) = p^2 r(X) + p f(X) s(X) + f(X)^2 t(X),$$

where $r(X)$, $s(X)$ and $t(X) \in Z[X]$. As

$$F_{p^e}(X) = X^{(p-1)p^{e-1}} + \cdots + X^{p^{e-1}} + 1,$$

it holds

$$p = F_{p^e}(1) = F_{p^e}(\eta^m) = p^2 r(\eta) + p f(\eta) s(\eta) + f(\eta)^2 t(\eta).$$

As p is not ramified at $Q(\eta)$, it holds $p \notin \mathfrak{p}^2$. But the right hand side is in $\mathfrak{p}^2$. This is a contradiction. This shows $F_{p^e}(X^m) \notin \mathfrak{m}^2$, i.e., $F_n(X) \notin \mathfrak{m}^2$.

TÔHOKU UNIVERSITY

Reference

[1] O. Zariski and P. Samuel: Commutative algebra, van Nostrand.