International Journal of Engineering, Science and Mathematics
Vol. 5 Issue 4, December 2016
ISSN: 2320-0294 Impact Factor: 6.238
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A STUDY ON RINGS OF INTEGERS AND THEORY OF FACTORIZATION

Seema
Research Scholar, Calorx Teachers' University
Ahmedabad (India)

Let *A* be an integral domain, and let *L* be a field containing *A.* An element *a* of *L* is said to be *integral* over *A* if it is a root of a *monic* polynomial with coefficients in *A*, i.e., if it satisfies an equation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

THEOREM 5.1 *The elements of L integral over A form a ring.* I shall give two proofs of this theorem. The first uses Newton's theory of symmetric polynomials and a result Eisenstein, and the second is Dedekind's surprisingly modern proof, which avoids symmetric polynomials.

FIRST PROOF THAT THE INTEGRAL ELEMENTS FORM A RING

A polynomial $P(X_1,\ldots,X_r) \in A[X_1,\ldots,X_r]$ is said to be *symmetric* if it is unchanged when its variables are permuted, i.e., if $P(X_{\sigma(1)},\ldots,X_{\sigma(r)}) = P(X_1,\ldots,X_r), \quad \text{all } \sigma \in \mathrm{Sym}_r.$

For example $$S_1 = \sum X_i, \quad S_2 = \sum_{i<j} X_iX_j, \quad \ldots, \quad S_r = X_1\cdots X_r,$$ are all symmetric.

These particular polynomials $P(X_1,\ldots,X_r)\ in\ A[X_1,\ldots,X_r]$ are called the *elementary symmetric polynomials.*

THEOREM 2.2 ***(Symmetric function theorem)*** *Let A be a ring. Every symmetric polynomial is equal to a polynomial in the symmetric elementary polynomials with coefficients in A, i.e.* $P \in A[S_1,\ldots,S_r]$,

PROOF. We define an ordering on the monomials in the X_i by requiring that $X_1^{i_1}X_2^{i_2}\cdots X_r^{i_r} > X_1^{j_1}X_2^{j_2}\cdots X_r^{j_r}$ if either

$$i_1 + i_2 + \cdots + i_r > j_1 + j_2 + \cdots + j_r$$

or equality holds and, for some *s*,

$$i_1 = j_1, \ldots, i_s = j_s, \text{ but } i_{s+1} > j_{s+1}.$$

Let $X_1^{k_1}\cdots X_r^{k_r}$ be the highest monomial occurring in P with a coefficient $c \neq 0$. Because P is symmetric, it contains all monomials obtained from $X_1^{k_1}\cdots X_r^{k_r}$ by permuting the X's. Hence $k_1 \geq k_2 \geq \cdots \geq k_r$.

Clearly, the highest monomial in S_i is $X_1\cdots X_i$, and it follows easily that the highest monomial in $S_1^{d_1}\cdots S_r^{d_r}$ is

$$X_1^{d_1+d_2+\cdots+d_r}X_2^{d_2+\cdots+d_r}\cdots X_r^{d_r}.$$

Therefore

$$P(X_1,\ldots,X_r)-cS_1^{k_1-k_2}S_2^{k_2-k_3}\cdots S_r^{k_r} < P(X_1,\ldots,X_r).$$

We can repeat this argument with the polynomial on the left, and after a finite number of steps, we will arrive at a representation of P as a polynomial in $S_1,\ldots,S_r$.

Let $f(X)=X^n+a_1X^{n-1}+\cdots+a_n \in A[X]$, and let $\alpha_1,\ldots,\alpha_n$ be the roots of f(X) in some ring containing A, so that $f(X)=\prod(X-\alpha_i)$ in the larger ring. Then

$$a_1=-S_1(\alpha_1,\ldots,\alpha_n),\quad a_2=S_2(\alpha_1,\ldots,\alpha_n),\quad \ldots,\quad a_n=\pm S_n(\alpha_1,\ldots,\alpha_n).$$

Thus the *elementary* symmetric polynomials in the roots of *f(X)* lie in *A*, and so the theorem implies that *every* symmetric polynomial in the roots of *f(X)* lies in *A*.

PROPOSITION 2.3 *Let A be an integral domain, and let be* Ω *an algebraically closed field containing A. If* $\alpha_1,\ldots,\alpha_n$ *are the roots in* Ω *of a monic polynomial in* $A[X]$*, then any* $g(\alpha_1,\ldots,\alpha_n)$ *polynomial in the* or, *with coefficients in A is a root of a monic polynomial in* $A[X]$

PROOF. Clearly

$$h(X)\stackrel{\text{def}}{=}\prod_{\sigma\in \mathrm{Sym}_n}(X-g(\alpha_{\sigma(1)},\ldots,\alpha_{\sigma(n)}))$$

is a monic polynomial whose coefficients are symmetric polynomials in the α_i, and therefore lie in *A*. But $g(\alpha_1,\ldots,\alpha_n)$ is one of its roots.

We now prove Theorem 5.1. Let α_1 and α_2 be elements of *L* integral over *A*. There exists a monic polynomial in *A [X]* having both α_1 and α_2 as roots. We can now apply with equal to $g(\alpha_1,\ldots)$ to $\alpha_1\pm\alpha_2$ or $\alpha_1\alpha_2$ deduce that these elements are integral over A.

DEDEKIND'S PROOF THAT THE INTEGRAL ELEMENTS FORM A RING

PROPOSITION 5.1 *Let L be a field containing A. An element a of L is integral over A if and only if there exists a nonzero finitely generated A-sub module of L such that* $\alpha M \subset M$ *(in fact we can take* $M=A[\alpha]$*, the A-sub algebra generated by* α*).*

PROOF. $\Rightarrow$: Suppose

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

Then the A-submodule M of L generated by $1, \alpha, \ldots, \alpha^{n-1}$ has the property that $\alpha M \subset M$ $\Leftarrow$: We shall need to apply Cramer's rule. As usually stated (in linear algebra courses) this says that, if

$$\sum_{j=1}^{m} c_{ij}x_j = d_i, \quad i = 1, \ldots, m,$$

Then

$$x_j = \det(C_j)/\det(C)$$

where $C = (c_{ij})$ and C_j is obtained from C by replacing the elements of the yth column with the *djS.* When one restates the equation as

$$\det(C)\cdot x_j = \det(C_j)$$

it becomes true over any ring (whether or not det(C) is
invertible). The proof is elementary— essentially it is what you wind up with when you eliminate the other variables (try it for m = 2). Alternatively, expand out

$$\det C_j = \begin{vmatrix} c_{11} & \cdots & \sum c_{1j}x_j & \cdots & c_{1m} \\ \vdots & & \vdots & & \vdots \\ c_{m1} & \cdots & \sum c_{mj}x_j & \cdots & c_{mm} \end{vmatrix}$$

using standard properties of determinants. Now let M be a nonzero A-module in L such that $\alpha M \subset M$, and let $v_1, \ldots, v_n$ be a finite set of generators for M. Then, for
each i ,
$\alpha v_i = \sum a_{ij}v_j$, some $a_{ij} \in A.$ We can rewrite this system of equations as

$$\begin{aligned} (\alpha - a_{11})v_1 - a_{12}v_2 - a_{13}v_3 - \cdots &= 0 \\ -a_{21}v_1 + (\alpha - a_{22})v_2 - a_{23}v_3 - \cdots &= 0 \\ \cdots &= 0. \end{aligned}$$

Let C be the matrix of coefficients on the left-hand side.

Then Cramer's rule tells us that $\det(C)\cdot v_i = 0$ for all. Since at least one v_i is nonzero and we are working inside the field L, this implies that det(C) = 0. On expanding out the determinant, we obtain an equation

$$\alpha^n + c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n = 0, \quad c_i \in A.$$

We now prove Theorem 5.1. Let or and β be two elements of L integral over A. and let M and N be finitely generated Amodules in L such that aM c M and $\beta N \subset N$. Define

$$MN = \left\{ \sum m_i n_i \mid m_i \in M, \quad n_i \in N \right\}$$

Then:

1. MN is an .4-submoduIe of *L* (easy);

2. it is finitely generated because, if $\{e_1,\ldots,e_m\}$ generates M

and $\{f_1,\ldots,f_n\}$ generates N, then $\{e_1 f_1,\ldots,e_i f_j,\ldots,e_m f_n\}$ generates

MN;

3. it is stable under multiplication by $\alpha\beta$ and by $\alpha \pm \beta$ We can now apply (5.1) to deduce that $\alpha\beta$ and $\alpha \pm \beta$ are integral over *A.*

RINGS OF INTEGERS ARE FINITELY GENERATED

We now show that $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module.

PROPOSITION 5.2 *Let A be an integrally closed integral domain with field of fractions K. and let B the integral closure of A in a separable extension L of K of degree m. There exists free Asubmodules M imd* M' *of L such that*

$$M \subset B \subset M' \quad \textbf{(6)}$$

Therefore, B is a finitely generated A-module if A is Noetherian. imd it is free of nuik m if A is a principal ideal domain.

PROOF. Let $\{\beta_1,\ldots,\beta_m\}$ be a basis for *L* over *K.* There exists a nonzero $d \in A$ such that $d \cdot \beta_i \in B$ for all. Clearly $\{d \cdot \beta_1,\ldots,d \cdot \beta_m\}$ is still a basis for *L* as a vector space over K. and so we may assume to begin with that each $\beta_i \in B$. Because the trace pairing is nondegenerate. there is a "dual" basis $\{\beta'_1,\ldots,\beta'_m\}$ of *L* over *K* such that $\mathrm{Tr}(\beta_i \cdot \beta'_j) = \delta_{ij}$. We shall show that

$$A\beta_1 + A\beta_2 + \cdots + A\beta_m \subset B \subset A\beta'_1 + A\beta'_2 + \cdots + A\beta'_m.$$

Only the second inclusion requires proof. Let $\beta \in B.$ Then β can be written uniquely as a linear combination $\beta = \sum b_j \beta'_j$ of the β'_j with coefficients $b_j \in K$, and we have to show that each $b_j \in A.$ As β_i and β are in B. so also is $\beta \cdot \beta_i$, and so. But

$$\mathrm{Tr}(\beta \cdot \beta_i) = \mathrm{Tr}(\sum_j b_j \beta'_j \cdot \beta_i) = \sum_j b_j \,\mathrm{Tr}(\beta'_j \cdot \beta_i) = \sum_j b_j \cdot \delta_{ij} = b_i.$$

Hence $b_i \in A$

If A Noetherian, then M' is a Noetherian y4-module, and so *B* is finitely generated as an A-module. If A is a principal ideal domain, then *B* is free of $\mathrm{rank} \leq m$ because it is contained in a free A -module of rank m, and it has $\mathrm{rank} \geq m$ because it contains a free A-module of rank m.

COROLLARY 5.1 *The ring of integers in a number field L is the largest subring that is finitely generated as a* $\mathbb{Z}$ *-module.* PROOF. We have just seen that $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$ - module.

Let B be another subring of L that is finitely generated as a $\mathbb{Z}$ -module; then every element of B is integral over $\mathbb{Z}$ (by 5.1). and so $B \subset \mathcal{O}_L$.

REMARK (a) The hypothesis that *L/K* be separable is necessary to conclude that *B* is a finitely generated Amodule (we used that the trace pairing was non degenerate).

However it is still true that the integral closure of $k[X]$ in any finite extension of $k(X)$ (not necessarily separable) is a finitely generated $k[X]$ module.

(b) The hypothesis that A be a principal ideal domain is necessary to conclude from (6) that *B* is a free A-module —there do exist examples of number fields L/K such that $\mathcal{O}_L$ is not a free $\mathcal{O}_K$ -module.

(c) Here is an example of a finitely generated module that is not free. Let $A = \mathbb{Z}[\sqrt{-5}]$ and consider the A-modules $(2) \subset (2, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$.

Both (2) and $\mathbb{Z}[\sqrt{-5}]$ are free $\mathbb{Z}[\sqrt{-5}]$ -modules of rank 1, but $(2, 1+\sqrt{-5})$ is *not* a free $\mathbb{Z}[\sqrt{-5}]$ -module of rank 1, because it is not a principal ideal. In fact, it is not a free module of any rank.

DEFINITION When *K* is a number field, a basis $\alpha_1, \ldots, \alpha_m$ for $\mathcal{O}_K$ as a $\mathbb{Z}$ -module is called an *integral basis* for *K*.

REMARK We retain the notations of the proposition and its proof.

(a) Let $C = \sum A\beta_i \subset B$, with β_i a basis for *L* over *K*. Define

$$C^* = \{\beta \in L \mid \mathrm{Tr}(\beta\gamma) \in A \text{ for all } \gamma \in C\}$$

By linearity,

$$\beta \in C^* \iff \mathrm{Tr}(\beta\beta_i) \in A \text{ for } i = 1, \ldots, m \quad \textbf{9}$$

and it follows that

$$C^* = \sum A\beta_i'$$

Thus we have:

$$C = \sum A\beta_i \subset B \subset \sum A\beta_i' = C^*$$

(b) Wrrite $L = \mathbb{Q}[\beta]$ with $\beta \in B$, and let $f(X)$ be the minimum polynomial of β . Let $C = \mathbb{Z}[\beta] = \mathbb{Z}1 + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{m-1}$. We want to find C^* One can show that

$$\mathrm{Tr}(\beta^i / f'(\beta)) = \begin{cases} 0 & \text{if } 0 \le i \le m-2 \\ 1 & \text{if } i = m-1 \end{cases}$$

(these formulas go back to Euler). It follows from this that $\det(\mathrm{Tr}(\beta^i \cdot \beta^j / f'(\beta)) = (-1)^m$ (the only term contributing to the determinant is the product of the elements on the *other* diagonal). If $\beta_1', \ldots, \beta_m'$ is the dual basis to $1, \beta, \ldots, \beta^{m-1}$, so

that $\mathrm{Tr}(\beta^i \cdot \beta'_j) = \delta_{ij}$, then $\det(\mathrm{Tr}(\beta^i \cdot \beta'_j)) = 1$

On comparing these formulas, one sees that the matrix relating the family

$$\{1/f'(\beta), \ldots, \beta^{m-1}/f'(\beta)\}$$

to the basis

$$\{\beta'_1, \ldots, \beta'_m\}$$

has determinant ± 1 , and so it is invertible in $M_n(A)$. Thus we see that C^* is a free *A*-module with basis $\{1/f'(\beta), \ldots, \beta^{m-1}/f'(\beta)\}$: $C = A[\beta] \subset B \subset f'(\beta)^{-1} A[\beta] = C^*$

UNIQUE FACTORIZATION

Factorization in subrings of number fields. Let *K* be a number field. Although there is much information which can be obtained just by considering K, answering many of the most interesting questions will require some sort of notion of factorization into primes. Factorization in *K* itself is not very interesting: every non-zero element is a unit, so there are no primes at all. In order to obtain these primes, we must somehow define a special subring of K this ring should have lots of primes, and factorizations in it should hopefully yield interesting arithmetic information.

EXAMPLE. As a first example of the useful of factorizations, let us solve the Diophantine equation

$$x^2 - y^2 = 105.$$

(When we speak of solving a Diophantine equation, we always mean that we are interested in solutions with $x, y \in \mathbb{Z}$, or occasionally $\mathbb{Q}$.) We can solve this equation by first factoring it as

$$(x + y)(x - y) = 105$$

Since both $x + y$ and $x - y$ are integers, we see that we are searching for pairs of integers $d = x + y,\ e = x - y$ such that $de = 105$. The fact that *x* and *y* are integers implies that *d* and *e* must be congruent modulo 2, so we are really looking for complimentary pairs of divisors of 105 which are congruent modulo 2. These pairs (up to reordering and negation) are

$$(d, e) = (105, 1), (35, 3), (21, 5), (15, 7);$$

they yield the solutions

$$(x, y) = (53, 52), (19, 16), (13, 8), (11, 4)$$

and their negatives. This example illustrates the usefulness of factorizations for solving Diophantine equations. On the other hand, when one has an equation like $x^2 + y^2 = p$ which

cannot be factored over $\mathbb{Z}$, it becomes necessary to add additional numbers with which to factor. In this case, $x^2 + y^2$ does factor over $\mathbb{Z}[i]$

The question, then, is which subring. We take as our model the subring $\mathbb{Z}$ of the number field $\mathbb{Q}$. Of course, we have a very good theory of factorization in $\mathbb{Z}$: every nonzero $n \in \mathbb{Z}$

factors uniquely as a product

$$n = \pm p_1^{e_1} \cdots p_k^{e_k}$$

where the p_i are distinct positive primes and all $e_i \geq 0$. This sort of factorization actually extends to the field $\mathbb{Q}$: any nonzero rational number $\frac{m}{n} \in \mathbb{Q}$ can be uniquely written as a product

$$\frac{m}{n} = \pm p_1^{e_1} \cdots p_k^{e_k}$$

where now we allow the e_i to be negative as well. Of course, the p_i are not really prime in $\mathbb{Q}$, but so long as we remember that they come from $\mathbb{Z}$ we can still consider them as distinguished elements to be used in factorizations. In any event, note that this sort of factorization shows that we have an isomorphism

$$\mathbb{Q}^* \cong \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}$$

where the direct sum is over all positive primes *p* of $\mathbb{Z}$. It is probably worth pausing a moment, here to clarify the sign issue. In $\mathbb{Z}$ we have two "copies" *p* and —*p* of each prime. They behave exactly the same in factorizations (the sign absorbing any changes), and there is no real reason to prefer one over the other. For the time being just assume that we have chosen one of them to use in factorizations; in the case of $\mathbb{Z}$ss , the positive primes are the natural choice but later on, when we have rings with lots of non-trivial units, there will be no obvious natural choices.

Fortunately, all of this confusion will go away as soon as we begin working with ideals rather than elements.

Returning to the previous discussion of factorization in Z, our first requirement must be that we have some sort of good factorization theory in our special subring R of K. We shall see later that it is unreasonable to ask for unique factorization, but we would like something close.

First condition (vague): *R* should have a good theory of factorization.

Our second requirement should be that the factorizations in *R* should extend to *K* in some way. The easiest way to insure this is to require that *K* be the *field of fractions* of *R*; this just means that every element of *K* can be written as a quotient of two elements of *R*. In particular, the subring of *K*, while a wonderful ring in many ways, has field of fractions, so it is not suitable for a theory of factorization in any number field larger than

Second condition: The field of fractions of *R* should be *K*. We will in fact obtain a stronger version of the second condition, and since it is easier to check we state it as well.

Second condition (strong form): Every $\alpha \in K$ can be written as α'/n where $\alpha' \in R$ and $n \in \mathbb{Z}$

All of the above conditions amount to asking that *R* be "big enough" this is clear for the second condition, while for the first we will see that in order to get a good factorization theory one must not leave out too many elements of K.

Now, it happens that $\mathbb{Q}$ has lots of subrings with all of $\mathbb{Q}$ as field of fractions. For example, for any set of primes *S* we have the ring.

$$S^{-1}\mathbb{Z} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \text{all prime factors of } b \text{ are in } S \right\}$$

In terms of unique factorization in $\mathbb{Z}$, rational numbers are in $S^{-1}\mathbb{Z}$ if and only if they can be written as $\pm p_1^{e_1} \cdots p_k^{e_k}$

where we allow e_i to be any integer for $p_i \in S$, but we require e_i to be positive if $p_i \notin S$of course, these rings seem somewhat contrived; we are really just adding some denominators to $\mathbb{Z}$ in fact, it is easy to see that all $p \in S$ are now units in $S^{-1}\mathbb{Z}$ so the primes of $S^{-1}\mathbb{Z}$ are just the primes of $\mathbb{Z}$not in 5. Thus factorizations into primes of $S^{-1}\mathbb{Z}$ contains less information than those in $\mathbb{Z}$ Somehow, then, in order to get the most information, we want to choose for R the smallest subring of *K* which satisfies the first two conditions.

Taking advantage of our knowledge that $\mathbb{Z}$ is a good prototype for i one possibility for this third condition is to require that $R \cap \mathbb{Q} = \mathbb{Z}$ *Third, condition:* $R \cap \mathbb{Q} = \mathbb{Z}$

Our goal, then, is to find a good interpretation of the first condition, and then we will hope that there is a natural subring of *K* satisfying the three conditions. First attempts. In order to help us figure out what interpretations to give to our first condition, let us begin by making some guesses. Let *K* be a quadratic number field.

We know that we can write $K = \mathbb{Q}(\sqrt{d})$ for a unique squarefrce integer *d.* Let us take our guess for the special subring to be $R = \mathbb{Z}[\sqrt{d}]$.

Now, while there are many other $d' \in \mathbb{Q}$such that $K = \mathbb{Q}(\sqrt{d'})$, this ring *R* has several things recommending it. First of all, if d' is not an integer, then $d' \in \mathbb{Z}[\sqrt{d'}] \cap \mathbb{Q}$, so this intersection is larger than $\mathbb{Z}$; this would violate our third condition. Also, if d' is a non-squarefree integer, then we can write $d' = e^2 d$,so $\sqrt{d'} \in R$ but $\sqrt{d} \notin \mathbb{Z}[\sqrt{d'}]$

Thus $\mathbb{Z}[\sqrt{d'}]$ seems to missing the element $\sqrt{d}$ which it really ought to contain, while R does not appear to be missing anything. (Later we will see that sometimes R is missing some non-obvious elements, but let us not worry about, this yet.) Considering all of this, then, $\mathbb{Z}[\sqrt{d}]$ seems to be the most natural choice for special subring *R.*

As a second example, take $K = \mathbb{Q}(\zeta_m)$. This time there is really only one obvious ring to write down, that being $R = \mathbb{Z}[\zeta_m]$ (Note that *R* is independent of the choice of primitive m^{th} root of unity ζ_m since every primitive m^{th} root of unity is a power of every other one. One can also check that if m is odd, then $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\zeta_{2m}]$, so that we have defined the same ring no matter which m is used to define *K.)* So for lack of any better choices, we will take $R = \mathbb{Z}[\zeta_m]$ to be our guess for $\mathbb{Q}(\zeta_m)$

The astute reader will have noticed that we have now made two different choices for the special subring of $K = \mathbb{Q}(\sqrt{-3})$. On the one hand, *K* is a quadratic field, so we have chosen $R = \mathbb{Z}[\sqrt{-3}]$. On the other hand, *K* is also a cyclostome field:

we have $K = \mathbb{Q}(\zeta_3)$, since

$$\zeta_3 = \frac{-1 + \sqrt{-3}}{2}.$$

In this case we have the choice $R' = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, which is actually larger than *R*. Right away we see that one of these must be wrong. We will figure out which one it is a bit later.

Ignoring that issue, note that at the very least these choices all satisfy the strong form of our second condition, and one can show without too much difficulty that they satisfy the third condition. The main remaining consideration is the factorization condition.

RINGS OF INTEGERS IN CYCLOTOMIC FIELDS

Let *p* be a rational prime and let $K = \mathbb{Q}(\zeta_p)$. We write ζ for ζ_p for this section.

Recall that *K* has degree $\varphi(p) = p - 1$ over $\mathbb{Q}$. We wish to show that $\mathcal{O}_K = \mathbb{Z}[\zeta]$

Note that ζ is a root of $x^p - 1$, and thus is an algebraic integer; since $\mathcal{O}_K$ is a ring we have that $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$. We need to show the other inclusion.

Following , we give a proof without assuming unique factorization of ideals. We begin with some norm and trace computations. Let *j* be any integer. If *j* is not divisible by p, then ζ^j is a primitive p^{th} root of unity, and thus its conjugates are $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Therefore

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta^j) = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = \Phi_p(\zeta) - 1 = -1.$$

If *p* does divide j, then $\zeta^j = 1$, so it has only the one conjugate 1, and

$$\mathrm{Tr}_{K/\mathbb{Q}}(\zeta^j) = p - 1$$

By linearity of the trace, we find that

$$\mathrm{Tr}_{K/\mathbb{Q}}(1 - \zeta) = \mathrm{Tr}_{K/\mathbb{Q}}(1 - \zeta^2) = \cdots = \mathrm{Tr}_{K/\mathbb{Q}}(1 - \zeta^{p-1}) = p.$$

We also need to compute the norm of $1 - \zeta$. For this, we use the factorization

$$x^{p-1} + x^{p-2} + \cdots + 1 = \Phi_p(x) = (x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{p-1});$$

plugging in *x* = 1 shows that

$$p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}).$$

Since the $1 - \zeta^j$ are the conjugates of $1 - \zeta$, this shows that $\mathrm{N}_{K/\mathbb{Q}}(1 - \zeta) = p.$

The key result for determining the ring of integers $\mathcal{O}_K$ is the following. Lemma 4.1.

$$(1 - \zeta)\mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$$

PROOF. We saw above that *p* is a multiple of $1 - \zeta$ in $\mathcal{O}_K$, so the inclusion

$$(1 - \zeta)\mathcal{O}_K \cap \mathbb{Z} \supseteq p\mathbb{Z}$$

is immediate. Suppose now that the inclusion is strict.

Since $(1-\zeta)\mathcal{O}_K \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ (check the definition) containing $p\mathbb{Z}$ and $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, we must have

$$(1-\zeta)\mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}.$$

Thus we can write

$$1 = \alpha(1-\zeta)$$

for some $\alpha \in \mathcal{O}_K$. That is, $1-\zeta$ is a unit in $\mathcal{O}_K$. But this is impossible by Lemma 1.9, since we know that $1-\zeta$ has norm *p*, while units have norm ± 1. This is a contradiction, which proves the lemma.

Corollary 5.2. *For any* $\alpha \in \mathcal{O}_K$,

$$\mathrm{Tr}_{K/\mathbb{Q}}((1-\zeta)\alpha) \in p \cdot \mathbb{Z}$$

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}((1-\zeta)\alpha) &= \sigma_1((1-\zeta)\alpha) + \cdots + \sigma_{p-1}((1-\zeta)\alpha) \\ &= \sigma_1(1-\zeta)\sigma_1(\alpha) + \cdots + \sigma_{p-1}(1-\zeta)\sigma_{p-1}(\alpha) \\ &= (1-\zeta)\sigma_1(\alpha) + \cdots + (1-\zeta^{p-1})\sigma_{p-1}(\alpha)\end{aligned}$$

where the σ_i are the complex embeddings of *K* (which we are really viewingas automorphisms of *K)* with the usual ordering. Furthermore, by Exercise $1-\zeta^j$ is a multiple of $1-\zeta$in $\mathcal{O}_K$ for every $j \neq 0$. Thus

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha(1-\zeta)) \in (1-\zeta)\mathcal{O}_K.$$

Since the trace is also a rational integer, Lemma completes the proof. Proposition 5.3. *Let p be a prime number and let* $K = \mathbb{Q}(\zeta_p)$ *be the pth cyclotomic field. Then*

$$\mathcal{O}_K = \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[x]/(\Phi_p(x));$$

thus $1, \zeta_p, \ldots, \zeta_p^{p-2}$ *is an integral basis for* $\mathcal{O}_K$

Proof. Let $\alpha \in \mathcal{O}_K$ and write

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

with $a_i \in \mathbb{Q}$. Then

$$\alpha(1-\zeta) = a_0(1-\zeta) + a_1(\zeta-\zeta^2) + \cdots + a_{p-2}(\zeta^{p-2}-\zeta^{p-1}).$$

By the linearity of the trace and our above calculations we find that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha(1-\zeta)) = pa_0.$$

So $a_0 \in \mathbb{Z}$.

Next consider the algebraic integer

$$(\alpha - a_0)\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-3};$$

this is an algebraic integer since $\zeta^{-1} = \zeta^{p-1}$ is. The same argument as above shows that $a_1 \in \mathbb{Z}$, and continuing in this way we find that all of the a_i are in $\mathbb{Z}$. This completes the proof.

One can use an almost identical proof in the case where ζ is a p^k-root of unity for some k. The case of ζ_m where m has multiple prime factors is usually handled by a general lemma on rings of integers in compositums of number fields.

REFERENCES

- Avigad, Jeremy (2006). \Methodology and metaphysics in the development of Dedekind's theory of ideals". In: The Architecture of Modern Mathematics. Ed. by Jose Ferreiros and Jeremy Gray. Oxford University Press, pp. 159{186 (cit. on pp. 8, 30).
- G.Greaves, Sieves in Number Theory. Results in Mathematics and Related Areas (3), 43. Springer-Verlag, Berlin, 2001.
- Gabor Ivanyos, Marek Karpinski, Lajos Ronyai, and Nitin Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. CoRR, abs/0811.3165, 2008. 30
- H.Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105
- H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. University Press of Cambridge, 2001.
- Harper, M., and Murty, R., Euclidean rings of algebraic integers, *Canadian Journal of Mathematics*, **56**(1), (2004), 71-76.
- J. A. Buchmann and H. W. Lenstra, Jr., Approximating rings of integers in number fields, J. Th_eor. Nombres Bordeaux 6 (1994), no. 2, 221{260. MR 1360644 (96m:11092)
- J.W.S. Cassels, Global fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42-84.
- Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc. 139, No. 9: 3025-3038, 2011.
- Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)
- M.Artin, Algebra, Prentice Hall Inc., Englewood Clients, NJ, 1991. MR 92g:00001
- Michael Atiyah and Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.
- Mollin, Richard: Algebraic Number Theory. Chapman and Hall/CRC Press. 1999
- Murty, R., *Problems in Analytic Number Theory*, GTM/RIM 206, Springer-Verlag, 2001
- Ono, Takashi: An Introduction to Algebraic Number Theory. Plenum Publishing Corporation. 1990