Unique Factorization of Ideals In Finite Algebraic Number Fields

Ellis Ballard Boal

Unique Factorization [illegible]

In Finite Algebraic [illegible]

An Honors Paper for the Department of Mathematics

by

Ellis [illegible]

Bowdoin College, 1966

Table of Contents

Errata

page 2 in diagram

Notice that K is isomorphic to some subset of $\not{\alpha}$: if $\alpha \in K$, then α satisfies an equation $f(x)$ in $\not{\alpha}[x]$. But since $\not{\beta}$ is algebraically (i.e. integrally) closed, and $\not{\alpha} \subseteq \not{\beta}$, some element α' of $\not{\beta}$ satisfies $f(x)$ ... So $\sigma : \alpha \mapsto \alpha'$ is an isomorphism.

page 34 proof of lemma 46

... statement that $[\beta] \in P$ requires a proof (for, suppose the conjugates of β are not in K; ... $\beta = \sqrt[3]{2}$ in $\not{\alpha}(\sqrt{-7})$). ... β ... plies

$$f(\beta) = \beta^m + c_{m-1}\beta^{m-1} + \dots + c_1\beta + c_0 = 0$$

$$c_0 = -\beta^m - c_{m-1}\beta^{m-1} - \dots - c_1\beta$$

... where $c_i \in \not{\alpha}$. So $c_0 \in P$. Let $[K : \not{\alpha}] = n$. If

$$f(\beta) = (x-\beta_0)\dots(x-\beta_m),$$

then

$$N(\beta) = (\beta_1 \cdots \beta_m)^{n/m} = (\dots c_0)^{n/m} \in P.$$

Since every prime ideal of I_K has a rational integer, lemmas 47, 48, and 49 are redundant; their only purpose in this paper was to show the existence of a rational integer in the prime ideal P,

in lemma 50. But this is shown here.

page 45 proof of lemma 48

The proof is incomplete: the existence of an inverse for a fractional ideal not an ideal of Z_K has not been shown. Let A be such a fractional ideal. Then by lemma 38, there is an element $b \in K$ such that bA is an ideal of Z_K. Then, for suitable prime ideals $P_1 \dots P_m$,

$$bA = P_1 \dots P_m$$

$$P_1^{-1} \dots P_m^{-1} bA = Z_K.$$

So

$$A^{-1} = b P_1^{-1} \dots P_m^{-1}$$

and $AA^{-1} = Z_K$. A^{-1} is a fractional ideal, because the P_i are.

pp 50-1 " h(x) has coefficients in Z_K."

Again, the conjugates of the α_i might not be in K (same example). But they are in Z_L, so the coefficients of h(x) are in Z_L. But they are also in K, because the coefficients of F(x) and $g_i(x)$ are. But $K \cap Z_L = Z_K$.

page 37 proof of lemma 35

Proof is false. The following proves the lemma. Assume there exists an ideal A for which the theorem is false. Let $\mathcal{M}$ be the set of ideals for which the theorem is false. $\mathcal{M}$ is not empty. By the Noetherian property, $\mathcal{M}$ has a maximal element, say E.

E is not prime. Let $E = (\alpha_1, \ldots, \alpha_s)$; let $\beta, \gamma \in E$, but $\beta, \notin E$, $\gamma \notin E$. Let

$$F = (\alpha_1, \ldots, \alpha_s, \beta)$$
$$G = (\alpha_1, \ldots, \alpha_s, \gamma)$$

$F, G \notin \mathcal{M}$, so there exist $P_1, \ldots, P_n$ such that $\pi_i P_i \subseteq F$, $F \subseteq P_i$ for all i; also there exist $Q_1, \ldots, Q_m$ such that $\pi_j Q_j \subseteq G$, $G \subseteq Q_j$ for all j. Then

$$\pi_{i,j} P_i Q_j \subseteq F \cdot G \subseteq E \subseteq F \subseteq P_i$$

$$\pi_{i,j} P_i Q_j \subseteq F \cdot G \subseteq E \subseteq G \subseteq Q_j$$

for all i. Thus the theorem actually does hold for E.

qed

page 47 lemma 47

The theorem is false by example: Let $K = \mathbb{Q}$, $Z_K = \mathbb{Z}$ then $f(x) = x^2 + 1 \in \mathbb{Z}[x]$, $x - i$ is a root of $f(x)$, and $f(x)/(x - i) = x + i \notin \mathbb{Z}[x]$.

However, the following lemma is true: If

$$f(x) = \delta_m x^m + \ldots + \delta_1 x + \delta_0$$

has algebraic integers (not necessarily in any finite

extension of Q) for coefficients, and π is one of its roots, then every coefficient of $f(x)/(x - \pi)$ has algebraic integers for coefficients. The proof goes through the same way. Similar changes in the corollary and in the following two lemmas are also required.

But, as noted above, these three lemmas are unnecessary to the proof of lemma 50, and so may be deleted from the paper anyway.

This paper sets out to prove a theorem, due to Dedekind, that there is unique factorization (UF) by prime ideals of ideals in the ring of algebraic integers in a finite field extension of the rational numbers. This will be proven in spite of the fact that there is generally not UF for elements in the ring.

The first chapter outlines the problem more explicitly. There are three conditions that the ring must be shown to satisfy in order to prove the theorem. These will be taken up in each of the next three chapters. The fifth chapter sidles up a few more preliminary notions, and the sixth shows a proof of the theorem. The sesixth shows some unexpected applications.

Throughout, the following symbols will be used: $\mathbb{Q}$ for the field of rational numbers, $\mathbb{Z}$ for the ordinary integers, or rational integers as they will always be called in the sequel, $\mathbb{R}$ for the real numbers, $\mathbb{C}$ the complex numbers, K for any finite field extension of $\mathbb{Q}$, and Z_K (to be defined below). Elements of K will be called algebraic numbers. Assume throughout that every ring is an integral domain.

Consider the field $\mathbb{Q}$ and any finite field extension K. Fields such as $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt[3]{5})$, or more generally $\mathbb{Q}(\sqrt[n]{m})$, where $m \in \mathbb{Z}$ satisfy this condition.

Notation: Designate the degree n of a field K over $\mathbb{Q}$ by $[K : \mathbb{Q}]$.

Note that $[K : \mathbb{Q}] = 1$ if and only if $K = \mathbb{Q}$. Suppose that $[K : \mathbb{Q}] = n$ and let $\alpha \in K$. Form the set $\{1, \alpha, \alpha^2, \ldots \alpha^N\}$.

The set is linearly dependent over $\mathbb{Q}$ since it contains $n + 1$ elements. Thus there exist in $\mathbb{Q}$ elements $a_0, \ldots, a_n$, not all $= 0$, such that

$$a_0 + a_1\alpha + \ldots + a_{N-1}\alpha^{N-1} + a_N\alpha^N = 0.$$

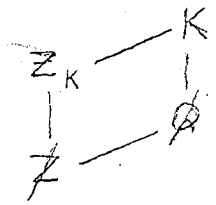
If a_n is the coefficient of the highest power of α that has a non-zero coefficient, divide the equation through by a_n to get a monic polynomial:

$$b_0 + b_1\alpha + \ldots + b_{r-1}\alpha^{r-1} + \alpha^r = 0$$

i.e. α satisfies some monic polynomial in $\mathbb{Q}[x]$ of degree $r \leq n$.

Example: if $K = \mathbb{Q}(i)$ and $\alpha = i$, since $[K : \mathbb{Q}] = 2$, i satisfies $x^2 + 1 \in \mathbb{Q}[x]$. Also, $(1 - i)$ satisfies $x^2 - 2x + 2$.

Define $Z_K = \{\alpha \in K \mid \alpha$ is the root of a monic polynomial in $\mathbb{Z}[x]\}$ Thus $i \in Z_{\mathbb{Q}(i)}$, but $\frac{1}{2}i$ is not. Note that $\mathbb{Z} \subseteq Z_K$ and $Z_K \subseteq K$. Elements of Z_K are henceforth called integers in K. We have now:



where $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ a subfield of K, and $\mathbb{Z}$ a subring in Z_K.

Now let $K = \mathbb{Q}(\sqrt{-5})$. All elements in K are of the form $a + b\sqrt{-5}$, $a, b \in \mathbb{Q}$. It can be shown[1] that $Z_K = \mathbb{Z}[\sqrt{-5}]$. Thus for instance, $9 = (9 + 0\sqrt{-5}) \in Z_K$. Note however that

$$9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}).$$

It can also be shown[2] that 3, $(2 + \sqrt{-5})$, and $(2 - \sqrt{-5})$ are all prime elements of $Z_{\mathbb{Q}(\sqrt{-5})}$ and not associated. Thus

$Z_{Q(\sqrt{-5})}$ is not a UF domain (UFD); this is the case for Z_K in general. However, according to the theorem there is a certain kind of UF that holds not for the elements, but for the ideals of Z_K; i.e. given an ideal A of Z_K, there exist a finite set of prime ideals $P_1, P_2, \ldots, P_n$ of Z_K such that $A = P_1 \cdots P_n$; moreover, this factorization is unique except for order.

Throughout this paper, it is enlightening to keep in mind the following example: It can be shown that any extension of degree 2 over $\mathbb{Q}$ is of the form

$$\mathbb{Q}(\sqrt{m})$$

where m is any square-free (i.e. having no squared factor), positive or negative, rational integer. Then, provided $m \equiv 2 \bmod 4$, or $m \equiv 3 \bmod 4$, Z_K is of the form:

$$\mathbb{Z}[\sqrt{m}]$$

For instance if $K = \mathbb{Q}(\sqrt{2})$, then $Z_K = \mathbb{Z}[\sqrt{2}]$. If $\alpha = 2 + \sqrt{2} \in K$, then α satisfies

$$f(x) = x^2 - 4x + 2 = 0.$$

For reference later in the paper, it should be noticed that the following are all the roots of f(x): $2 + \sqrt{2}$, $2 - \sqrt{2}$. Also the product of the two roots is $(2+\sqrt{2})\cdot(2-\sqrt{2}) = 2$.

II

The first task, before talking about ideals in Z_K, is to show that Z_K is in fact a ring. From this it will be discovered that Z_K is a finitely generated module over $\mathbb{Z}$ which will give (1) that Z_K is Noetherian. (as we shall see below).

Also it will be shown that (2) prime ideals in Z_K are maximal, and that (3) Z_K is integrally closed (to be defined below) in its quotient or fraction field. The theorem will then give the desired result. The demonstration that Z_K satisfies the three conditions will go in the order (3), (1), (2).

Definition: Let R,S be rings, $R \subseteq S$. Then $\theta \in S$ is said to be integral over R if θ satisfies a polynomial equation

$$a_0 + a_1 x + \ldots + a_{N-1} x^{N-1} + x^N = 0,$$

where $a_i \in R$; θ need not be in R; if R is a field, then θ is algebraic over R.

Thus for all $\alpha \in K$, α is algebraic over $\mathbb{Q}$. Since this is true, K is said to be algebraic over $\mathbb{Q}$.

If $\alpha \in K$, it may satisfy more than one monic polynomial over $\mathbb{Q}$. In this case, choose one, say p(x), of lowest degree.

Definition: p(x) so chosen is called a minimal polynomial for over $\mathbb{Q}$. p(x) is clearly irreducible, for otherwise α would satisfy a polynomial of lower degree.

Lemma 1: If $\alpha \in K$, then α has a unique minimal polynomial over $\mathbb{Q}$.

Proof: Let p(x) be a minimal polynomial and s(x) be any other polynomial satisfied by α. Since the polynomial ring $\mathbb{Q}[x]$ is Euclidean, there exist polynomials q(x), r(x) in $\mathbb{Q}[x]$ having the properties

$$s(x) = q(x) \cdot p(x) + r(x)$$

where deg r(x) < deg p(x), or r(x) = 0.

So

$$s(\alpha) = q(\alpha) \cdot p(\alpha) + r(\alpha)$$
$$0 = q(\alpha) \cdot 0 + r(\alpha)$$
$$0 = r(\alpha)$$

whence α satisfies $r(x)$. But deg $r(x) <$ deg $p(x)$ then contradicts the minimality of the degree of $p(x)$; this leaves only the possibility that $r(x) = 0$, and $s(x) = q(x) \cdot p(x)$. So $p(x) \mid s(x)$.

But if $s(x)$ is another minimal polynomial for α over $\mathbb{Q}$, the same argument gives $s(x) \mid p(x)$. Thus $s(x) = \pm p(x)$. But since both are monic, $s(x) = p(x)$.

qed

Corollary : The minimal polynomial of α divides any polynomial in $\mathbb{Q}[x]$ that α satisfies.

Lemma 2: If $f(x)$ and $g(x)$ are relatively prime in $\mathbb{Q}[x]$ they have no roots in common.

Proof: If $f(x)$, $g(x)$ are relatively prime in $\mathbb{Q}[x]$, then there exist $s(x)$, $t(x)$ such that

$$f(x)\, s(x) + g(x)\, t(x) = 1$$

If α is a common root, then $0 = 1$.

qed

Definition: An algebraic number is an algebraic integer if its minimal polynomial over $\mathbb{Q}$ has coefficients only in $\mathbb{Z}$. The term "algebraic integer" will occasionally be abbreviated to "integer".

Definition: A polynomial in $\mathbb{Z}[x]$ is primitive if its coef-

ficients are relatively prime; i.e. the highest common factor of all of them is 1.

Lemma 3: (Gauss' Lemma) The product of primitive polynomials is primitive.

Proof: Let $a_0 + a_1 X + \ldots + a_N X^N$ and $b_0 + b_1 X \ldots + b_m X^m$ be primitive, and suppose their product is $c_0 + c_1 X + \ldots + c_k X^k = c(x)$. Suppose the product is not primitive. Then some prime p divides every coefficient of c(x). Let a_i and b_j be the first coefficients in the two original polynomials that p does not divide (they must exist, since both polynomials are primitive).

Then by the formula for the product of two polynomials,

$$c_{i+j} = (a_0 b_{i+j} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0)$$

But p divides $a_0, \ldots, a_{i-1}, b_0, \ldots, b_{j-1}$ and c_{i+j}, so $(a_i \cdot b_j)$ is divisible by p.

But p prime implies that $p \mid a_i$ or $p \mid b_j$, contradicting the choice of a_i and b_j. Thus $c_0 + c_1 X + \ldots + c_k X^k$ has no common factor p for its coefficients, and is primitive.

qed

Lemma 4: Any $f(x) \neq 0 \in \mathbb{Q}[x]$ can be written uniquely as

$$f(x) = c_f \cdot f^*(x)$$

where $f^*(x)$ is primitive in $\mathbb{Z}[x]$ and $c_f > 0 \in \mathbb{Q}$.

Proof: Say $f(x) = a_N X^N + \ldots + a_1 X + a_0$, $a_i \in \mathbb{Q}$. Each a_i can be written (b_i/c), where c is the least positive common multiple of all denominators of the fractions a_i; b_i, $c \in \mathbb{Z}$. Then

$$f(x) = \frac{1}{c} (b_N X^N + \ldots + b_1 X + b_0)$$

Now factor out of the expression in parentheses the largest positive common factor b of all the b_i:

$$f(x) = \frac{b}{c}\left(b_N' x^N + \ldots + b_1' x + b_0' \right).$$

Let $\frac{b}{c} = c_f$, $\left(b_N' x^N + \ldots + b_1' x + b_0' \right) = f^*(x)$. Clearly $c_f > 0$, and $f^*(x)$ is primitive by construction.

For uniqueness, if $f(x) = c_f \cdot f^*(x) = c \cdot p(x)$ where $c_f, c > 0$, and $f^*(x)$, $p(x)$ are primitive, then $f^*(x) \mid p(x)$ and $p(x) \mid f^*(x)$, so $f^*(x) = \pm p(x)$; the $+$ sign must prevail since both c_f and c are positive.

qed

Lemma 5: If $\alpha \in K$ satisfies some monic polynomial $f(x)$ with coefficients in $\mathbb{Z}$ (i.e. if $\alpha \in Z_K$), then the minimal polynomial of α has coefficients only in $\mathbb{Z}$ (i.e. α is an algebraic integer).

Proof: Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$. By the corollary to lemma 1, $f(x) = q(x) \cdot p(x)$, where $q(x) \in \mathbb{Q}[x]$. Thus by lemma 4:

$$c_f \cdot f^*(x) = c_p \cdot c_q \cdot p^*(x) \cdot q^*(x),$$

where $f^*(x)$, $p^*(x)$, and $q^*(x)$ are primitive. Thus by lemma 3, $p^*(x) \cdot q^*(x)$ is primitive, and lemma 4 gives $f^*(x) = p^*(x) \cdot q^*(x)$. So

$$f(x) = c_f f^*(x) = c_f \cdot p^*(x) \cdot q^*(x).$$

Since $f(x)$ is monic, and thus primitive, $c_f = 1$:

$$f(x) = p^*(x) \cdot q^*(x).$$

$p^*(x)$ and $q^*(x)$ have coefficients in $\mathbb{Z}$ and must thus be monic since their product $f(x)$ is monic. But $p(x)$ is also monic. $p^*(x)$ monic and $p(x)$ monic give $c_p = 1$, and $p(x) = p^*(x)$ has coefficients in $\mathbb{Z}$.

qed

Thus if $\alpha \in Z_K$, α is an algebraic integer; conversely every algebraic integer $\beta \in K$ is in Z_K, and Z_K is exactly the set of all algebraic integers in K.

Lemma 6: The roots of an irreducible polynomial of degree n over $\mathbb{Q}$ are distinct.

Proof: Let $p(x)$ be the irreducible polynomial. It is well-known[4] that $p(x)$ splits over $\mathbb{Q}$; i.e. that

$$p(x) = a_0 (x - \pi_1) \cdots (x - \pi_N)$$

is a UF of $p(x)$, where the π_i are in $\mathbb{Q}$. So $p(x)$ has n roots and at most n distinct roots.

Suppose that two of them are the same; i.e.

$$p(x) = a_0 (x-\alpha)^2 \cdot g(x)$$

Take the derivative of both sides (derivative is defined as usual for polynomials in $\mathbb{Q}[x]$).

$$p'(x) = 2a_0 (x-\alpha) \cdot g(x) + a_0 (x-\alpha)^2 g'(x).$$

Notice that α is thus also a root of $p'(x)$. By corollary lemma 2, $p(x)$ and $p'(x)$ have a common factor. Since $p(x)$ is irreducible, it must be the common factor: $p(x) \mid p'(x)$. But this is impossible since $p'(x)$ is of lower degree than $p(x)$. Therefore, $p(x)$ must have distinct roots.

qed

Definition: Suppose $\Theta \in K$, and $p(x)$ is its minimal polynomial over $\mathcal{C}$, say of degree m. Then Θ is said to be of degree m over $\mathcal{C}$. The distinct roots (in $\mathcal{C}$) $\Theta_1, \ldots, \Theta_m$ of $p(x)$ where $\Theta = \Theta_1$ are called the distinct conjugates of Θ over $\mathcal{C}$.

Definition: a polynomial $g(\alpha_1, \ldots, \alpha_N)$ in $\mathcal{C}[x]$ is symmetric if it is unchanged by any of the $N!$ permutations of the variables $\alpha_1, \ldots, \alpha_N$.

Example: for $N = 3$, the polynomials $\alpha_1 + \alpha_2 + \alpha_3$ and $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1$ are symmetric.

Suppose that x is another variable, and

$$f(x) = (x-\alpha_1)\ldots(x-\alpha_N) = x^N - \sigma_1 x^{N-1} + \ldots (-1)^N \sigma_N.$$

Then

$$\sigma_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_N$$

$$\sigma_2 = \alpha_1\alpha_2 + \ldots + \alpha_1\alpha_N + \alpha_2\alpha_3 + \ldots + \alpha_2\alpha_N + \ldots + \alpha_{N-1}\alpha_N$$

$$\vdots$$

$$\sigma_i = \text{sum of all products of } i \text{ different } \alpha_j$$

$$\vdots$$

$$\sigma_N = \alpha_1\alpha_2 \ldots \alpha_N .$$

(This can be seen conceptually by arranging the factors vertically with the x's in one column, and the α_i in the other

$$\begin{matrix} (x-\alpha_1) \\ (x-\alpha_2) \\ (x-\alpha_3) \\ \vdots \\ (x-\alpha_N), \end{matrix}$$

and noting that the product $f(x)$ is the sum of all products of n elements, one taken from the pair in each row in the arrangement. There are 2^n such products.)

Definition: The above σ_i are called the elementary symmetric functions in $\alpha_1, \ldots, \alpha_N$

The following lemma is assumed without proof. It is a standard theorem on symmetric polynomials, and can be found in many sources.[5]

Lemma 7: Every symmetric polynomial in $x_1, \ldots, x_N$ over $\mathbb{Q}$ can be written as a polynomial over $\mathbb{Q}$ in the elementary functions $\sigma_1, \ldots, \sigma_N$. If the coefficients of the first polynomial are rational integers, so are the coefficients of the second.

qed

Example: for $n = 3$,

$$\begin{aligned} & x_1^2 + x_2^2 + x_3^2 \\ &= (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) \\ &= \sigma_1^2 - 2\sigma_2 . \end{aligned}$$

Lemma 8: Let $f(x) \in \mathbb{Q}[x]$ be of degree n with roots $r_1, \ldots, r_n$. Let $p(x_1, \ldots, x_n) \in \mathbb{Q}[x]$ be a symmetric polynomial. Then $p(r_1, \ldots, r_n) \in \mathbb{Q}$.

Proof: By lemma 7, $p(x_1, \ldots, x_n)$ is a polynomial over $\mathbb{Q}$ in $\sigma_1, \ldots, \sigma_N$. Thus $p(r_1, \ldots, r_n)$ is a polynomial over $\mathbb{Q}$ in $(r_1 + \ldots + r_n)$, $(r_1r_2 + r_1r_3 + \ldots + r_{n-1}r_n)$, $\ldots$, $(r_1r_2 \ldots r_n)$. Write $f(x)$ as

$$\begin{aligned} f(x) &= c_N x^N + c_{N-1} x^{N-1} + \ldots + c_1 x + c_0 \\ &= c_N (x^N - b_{N-1} x^{N-1} + b_{N-2} x^{N-2} - \ldots \pm b_0), \end{aligned}$$

so

$$\frac{f(x)}{c_n} = x^n - b_{n-1}x^{n-1} + b_{n-2}x^{n-2} - \ldots \pm b_0 .$$

But $(r_1 + \ldots + r_n)$, $(r_1r_2 + r_1r_3 + \ldots + r_{n-1}r_n)$ $\ldots$, $(r_1 \ldots r_n)$ are the unsigned coefficients b_i of $\frac{f(x)}{c_n}$, since r_i are the roots of $\frac{f(x)}{c_n}$; thus $b_i \in \mathbb{Q}$. Thus $p(r_1, \ldots, r_n) \in \mathbb{Q}$. qed

Example: Consider, $f(x) = 2x^2 - 7x + 7$, and $p(x_1, x_2)$ $x_1^2 + x_2^2$. The roots of $f(x)$ are $(7 \pm i\sqrt{7})/4$ and

$$p(r_1r_2) = \left(\frac{7 + i\sqrt{7}}{4}\right)^2 + \left(\frac{7 - i\sqrt{7}}{4}\right)^2$$
$$= \frac{21}{4} \in \mathbb{Q}$$

as predicted.

(ascending chain condition)

Lemma 9: If ACC holds on R, and M is a finite R-module, then ACC holds on every sub-module N of M.

Equivalent statement of lemma 9: If every ideal of R has a finite basis, and M is a finitely-generated R-module, then every sub-module N of M is a finitely-generated R-module.

Proof: (analogous to proof of Hilbert basis theorem) Let $M = (a_1, \ldots, a_h)$. Every element of N may be written in the form

$$\gamma = r_1 a_1 + \ldots + r_h a_h$$

where $r_i \in R$. In this expression, if the last $h - p$ coefficients are $= 0$, the expression is said to be of length $\leq p$.

Let $A_p = \{ r_p \in R \mid r_p$ is the coefficient of a_p in an expression $r_1 a_1 + \ldots + r_h a_h$ of length $\leq p$ in $N \}$. Show A_p is an ideal in R. Say s_p, $t_p \in A_p$; i.e. there exist

$$\alpha = s_1 a_1 + \ldots + s_p a_p$$

$$\beta = t_1 a_1 + \ldots + t_p a_p$$

in N. Then $\alpha - \beta = (s_1 - t_1)a_1 + \ldots + (s_p - t_p)a_p$ is an expression of length $\leq p$ in N; so $s_p - t_p \in A_p$. For all $y \in R$,

$$y\alpha = (ys_1)a_1 + \ldots + (ys_p)a_p$$

is an expression of length $\leq p$ in N; so $ys_p \in A_p$. Note that $0 \in A_p$. Thus A_p is an ideal in R.

A_p has a finite basis $(b_{p1}, \ldots, b_{ps_p})$. Every b_{pi} is the p^{th} coefficient of some expression $r_1 a_1 + \ldots + r_p a_p$ of length $\leq p$ in N. Call it

$$B_{pi} = r_{(pi)}a_1 + \ldots + r_{(pi)}a_{p-1} + b_{pi}a_p.$$

Show that the totality of all B_{pi}, where $1 \leq p \leq h$, $1 \leq i \leq s_p$, generate the sub-module N of M.

Every element γ of length $\leq p$ can be transformed to an expression δ of length $\leq p - 1$, by subtracting a linear combination of the B_{pi} determined as follows: if $\gamma = r_1 a_1 + \ldots + r_p a_p$ then r_p is in A_p, and thus can be represented as a certain linear combination of the b_{pi}, say

$$r_p = d_{p1}(b_{p1}) + \ldots + d_{ps_p}(b_{ps_p}).$$

Then $\delta = \gamma - d_{p1} B_{p1} - \ldots - d_{ps_p} B_{ps_p}$ is an expression of length $\leq p - 1$. It is clear that if δ can be represented as a linear combination of the B_{pi}, then so can γ. Thus induction on p can be invoked, noting that any expression of length ≤ 0 (there is only one; it is 0) can be expressed as a linear combination of the B_{pi}. Thus N is generated by the B_{pi}.

qed

Lemma 10: If ACC holds for ideals of a ring $R \subseteq S$, S a ring, then $\Theta \in S$ is integral over R if and only if all powers Θ^h of Θ belong to a finitely generated R-module $(a_1, \ldots, a_m)$ in S; i.e. for all h

$$\Theta^h = b_1 a_1 + \ldots + b_m a_m,$$

$a_i \in S$, $b_i \in R$.

Proof: Say Θ is integral over R. Then there are elements $r_i \in R$ such that

$$\Theta^m + r_{m-1}\Theta^{m-1} + \ldots + r_1\Theta + r_0 = 0,$$
$$\Theta^m = -r_{m-1}\Theta^{m-1} - \ldots - r_1\Theta - r_0$$

for some m. Thus Θ^m and consequently all higher powers of Θ can be represented as a linear combination of $\{1, \Theta, \ldots, \Theta^{m-1}\}$ i.e. $\Theta^h \in (1, \Theta, \ldots, \Theta^{m-1})$, for all h.

Conversely, say $\theta^h \in (a_1, \ldots, a_m) \subseteq S$ for all h. since ACC holds for ideals of R, ACC holds for sub-modules of $(a_1, \ldots, a_m)_\Lambda$ by lemma 9. Thus the chain of modules

$$(1,\theta) \subseteq (1,\theta,\theta^2) \subseteq \ldots$$

must contain non-distinct modules; i.e. there is a power θ^h of θ such that

$$\theta^h = r_{h-1}\theta^{h-1} + \ldots + r_1\theta + r_0$$
$$\theta^h - r_{h-1}\theta^{h-1} - \ldots - r_1\theta - r_0 = 0$$

so θ is integral over R.

qed

Lemma 11: Z_K is a subring of K.

Proof: It suffices to show that if $\alpha,\beta \in Z_K$ then $\alpha\beta$, $\alpha+\beta$, $\alpha-\beta \in Z_K$. Since ACC holds in Z the preceding lemma applies, letting $R = Z$ and $S = K$. (If a Z-module is generated by $c_1, \ldots, c_p$, call it $(c_1, \ldots, c_p)$.) Thus if $\alpha,\beta \in Z_K$

$$\alpha^h \in (a_1, \ldots, a_n) = A$$
$$\beta^h \in (b_1, \ldots, b_k) = B$$

for all powers α^h and β^h of α and β, for some a_i, $b_j \in K$. Are all powers of $\alpha\beta$, $\alpha+\beta$, $\alpha-\beta$ in some finitely generated Z-module? If so the lemma is proved. Let

$$M = (a_1b_1, \ldots, a_ib_j, \ldots, a_nb_k),$$

for all i, j (M is merely the product of the above two modules). Thus all powers $(\alpha\beta)^h = \alpha^h \cdot \beta^h$ of $\alpha\beta$ are in M, a finitely generated Z-module. Therefore $\alpha\beta$ is integral, i.e. in Z_K, by the preceding lemma.

For $\alpha \pm \beta$, note that

$$(\alpha \pm \beta)^h = \alpha^h \pm c_1 \alpha^{h-1}\beta + c_2 \alpha^{h-2}\beta^2 \pm \ldots$$
$$\ldots + c_{h-1}\alpha\beta^{h-1} \pm \beta^h,$$

and the $c_i \in \mathbb{Z}$. Let

$$L = (a_1, \ldots, a_n, b_1, \ldots, b_K, a_1 b_1, \ldots, a_i b_j, \ldots, a_n b_K)$$
$$= A + B + M.$$

Then, in $(\alpha \pm \beta)^h$, $\alpha^h \in A$, $\beta^h \in B$, and all the middle terms are in M; thus $(\alpha \pm \beta)^h \in L$ a finitely generated $\mathbb{Z}$-module. $(\alpha \pm \beta) \in Z_K$ and Z_K is a ring.

Lemma 12: $\mathbb{Z} = Z_K \cap \mathbb{Q}$. qed

Proof: Certainly $\mathbb{Z} \subseteq Z_K \cap \mathbb{Q}$. Suppose $\alpha \in Z_K$, $\alpha = \frac{p}{q}$ where $p, q \in \mathbb{Z}$, and p and q are relatively prime; then for $a_i \in \mathbb{Z}$

$$\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$
$$p^n + q a_{n-1} p^{n-1} + \ldots + q^{n-1} a_1 p + q^n a_0 = 0,$$

so $p^n \equiv 0 \bmod q$, or $q \mid p^n$.

But p and q are relatively prime, so p^n and q are relatively prime; yet $q \mid p^n$. Thus $q = 1$ and $\frac{p}{q} = p \in \mathbb{Z}$. whence $Z_K \cap \mathbb{Q} \subseteq \mathbb{Z}$.

So $Z_K \cap \mathbb{Q} = \mathbb{Z}$.

qed

Note that Z_K has the identity, and in fact is an integral domain (because K is). So it can reasonably be asked, "What is the fraction field of Z_K?"

Lemma 13: If $\alpha \in K$ then there exists $s \neq 0 \in \mathbb{Z}$ such that $s\alpha \in Z_K$

Proof: $\alpha \in K$ implies that α is algebraic over $\mathbb{Q}$ i.e. there are $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

But $a_i \in \mathbb{Q}$ implies $a_0 = \frac{r_0}{s_0}, \ldots, a_{n-1} = \frac{r_{n-1}}{s_{n-1}}$, where all s_i, $r_i \in \mathbb{Z}$, $s_i \neq 0$. Let

$$S = s_0 s_1 \ldots s_{n-1} = \prod_{i=0}^{n-1} s_i \in \mathbb{Z}.$$

Evaluate the minimal polynomial of α at α and multiply through by s^n:

$$s^n\alpha^n + s^n a_{n-1}\alpha^{n-1} + \ldots + s^n a_1\alpha + s^n a_0 = 0$$

$$(s\alpha)^n + s a_{n-1}(s\alpha)^{n-1} + \ldots + s^{n-1} a_1(s\alpha) + s^n a_0 = 0$$

and $(s^{n-i}a_i) \in \mathbb{Z}$ $\forall\, i$, $0 \leq i \leq n$. Thus $s\alpha \in Z_K$, where $s \in \mathbb{Z}$, $s \neq 0$.

qed

Corollary: The fraction field of Z_K is exactly K.

Proof: By the lemma, if $\alpha \in K$, then there exists $s \in \mathbb{Z}$, and $\beta \in Z_K$ such that $\alpha = \frac{\beta}{s}$. But s is $\in Z_K$ also, so α is in the field of fractions of Z_K, for all $\alpha \in K$. On the other hand, since $Z_K \subseteq K$, the fraction field of Z_K is certainly $\subseteq K$. Consequently the fraction field of Z_K and K are identical.

Definition: A ring R is said to be integrally closed in a ring S if the set of all elements of S that are integral over R is R itself.

Lemma 14: Z_K is integrally closed in its fraction field K.

Proof: It must be shown that if $\alpha \in K$ is integral over Z_K, then α is in Z_K, i.e. if

$$\alpha^n + \gamma_{n-1}\alpha^{n-1} + \ldots + \gamma_1 \alpha + \gamma_0 = 0$$

where $\gamma_i \in Z_K$ then $\alpha \in Z_K$. This equation states that α^n, and consequently all higher powers of α can be expressed linearly in terms of $1, \alpha, \ldots, \alpha^{n-1}$, with sums of products of powers of the γ_i as coefficients. But each $\gamma_i \in Z_K$; thus

$$\gamma_i^{m_i} = -r_0 - r_1\gamma_i - \ldots - r_{m_i-1}\gamma_i^{m_i-1}$$

for some m_i, and the $r_j \in \mathbb{Z}$. Thus all powers of γ_i can be expressed linearly in terms of $1, \gamma_i, \ldots, \gamma_i^{m_i-1}$ with coefficients in $\mathbb{Z}$; and all products of powers of γ_i can be expressed linearly in terms of products of the $1, \gamma_i, \ldots, \gamma_i^{m_i-1}$, with coefficients in $\mathbb{Z}$. There are a finite (though possibly quite large) number of these products. Call them $\delta_1, \delta_2, \ldots \delta_p$. Multiply each of the δ_k by $1, \alpha, \alpha^2, \ldots,$ and α^{n-1}. Then all powers of α can be expressed linearly in terms of the products $\delta_k \cdot \alpha_h$ together with $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients in $\mathbb{Z}$. Since $\mathbb{Z}$ is Noetherian, lemma 10 applies, and $\alpha \in Z_K$.

qed.

Note that if $\alpha \in Z_K$, then α is algebraic over Z_K; consequently $Z_K = \{\text{all algebraic integers in } K\} = \{\alpha \in K \mid \alpha \text{ is algebraic over } Z_K\}$.

III

One of the three premises for the theorem has been established, that of integral closure of Z_K in K. The next task is to show that as a module over $\mathbb{Z}$, Z_K is finitely generated; i.e. that there exist $\alpha_1, \ldots, \alpha_n \in Z_K$ such that for any $z \in Z_K$, z can be uniquely represented as

$$z = m_1 \alpha_1 + \ldots + m_n \alpha_n$$

where $m_i \in \mathbb{Z}$. This will give that Z_K is Noetherian.

Definition: An integral basis for K is any minimal set of generators $\{\alpha_1, \ldots, \alpha_n\}$ for Z_K as a finitely generated module over $\mathbb{Z}$, such that every element of Z_K can be represented uniquely as a linear combination of the $\{\alpha_1, \ldots, \alpha_n\}$.

Thus if K has an integral basis, then Z_K is a finitely generated module over $\mathbb{Z}$.

Lemma 15: An integral basis for K is a basis for K. (as a finite dimensional vector space over $\mathbb{Q}$.).

Proof: Suppose that $\{\beta_1, \ldots, \beta_n\}$ is an integral basis and $\alpha \in K$. By lemma 13 there is $r \neq 0 \in \mathbb{Z}$ such that $r\alpha \in Z_K$ Thus

$$r\alpha = b_1 \beta_1 + \ldots + b_n \beta_n$$

for suitable $b_i \in \mathbb{Z}$;

$$\alpha = \frac{b_1}{r} \beta_1 + \ldots + \frac{b_n}{r} \beta_n$$

where $\frac{b_i}{r} \in \mathbb{Q}$. So the α_i generate K. Are they linearly independent? Suppose

$$c_1 \beta_1 + \ldots + c_n \beta_n = 0$$

for $c_i \in \mathbb{Q}$. Multiply through by the least common multiple of the denominators

of the c_i and get

$$\alpha_1 \beta_1 + \ldots + \alpha_n \beta_n = 0,$$

where $\alpha_i \in \mathbb{Z} \subseteq \mathbb{Z}_K$.

By definition of integral basis, $a_i = 0$ for all i. Thus all $c_i = 0$, and the β_i are linearly independent over $\mathcal{K}$.

qed

Corollary: The number of elements in an integral basis is the degree of K over $\mathcal{K}$.

Definition: Let $\theta \in S$ a field extension of $\mathcal{K}$, and let θ be algebraic over $\mathcal{K}$. Then $\mathcal{K}(\theta)$, the smallest field containing both $\mathcal{K}$ and θ is called a simple algebraic extension of $\mathcal{K}$.

It is clear that $\mathcal{K}(\theta)$ consists of all quotients $f(\theta)/g(\theta)$, where $f(x)$, $g(x) \in \mathcal{K}[x]$, and $g(\theta) \neq 0$.

Lemma 16: If $\mathcal{K}(\theta)$ is a simple algebraic extension of $\mathcal{K}$, then $\{1, \theta, \ldots, \theta^{n-1}\}$ form a basis for $\mathcal{K}(\theta)$ as a vector space over $\mathcal{K}$, where n is the dimension of $\mathcal{K}(\theta)$ over $\mathcal{K}$.

Proof: Suppose $\alpha \in \mathcal{K}(\theta)$; then $\alpha = f(\theta)/g(\theta)$, $g(\theta) \neq 0$. Let $p(x)$ be the (irreducible) minimal polynomial for θ over $\mathcal{K}$. Then $p(x) \nmid g(x)$, for otherwise $g(\theta) = 0$; thus $p(x)$ and $g(x)$ are relatively prime. This means that there exist polynomials $s(x)$ and $t(x)$ such that

$$t(x) \cdot p(x) + s(x) \cdot g(x) = 1$$

$$t(\theta) \cdot p(\theta) + s(\theta) \cdot g(\theta) = 1$$

$$g(\theta) = 1/s(\theta)$$

So $\alpha = f(\theta)/g(\theta) = f(\theta) \cdot s(\theta)$

or say $\alpha = h(\theta)$

Now $h(x) = q(x) \cdot p(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg p(x) = n$.

But then

$$\alpha = h(\theta) = q(\theta)\cdot p(\theta) + r(\theta)$$
$$= r(\theta)$$

for all $\alpha \in \mathcal{K}(\theta)$.

It must still be shown that for given α, $r(\theta)$ is unique. Suppose $\alpha = r'(\theta)$. Then

$$0 = \alpha - \alpha = r(\theta) - r'(\theta)$$

But $\deg(r(x) - r'(x)) < n$, and θ satisfies no polynomial of degree $< n$. It follows that $r(x)$ and $r'(x)$ are identical.

Thus α has been uniquely expressed as a linear combination of $\{1, \theta, \ldots, \theta^{n-1}\}$ with coefficients in $\mathcal{K}$.

qed

The following lemma is not essential to the paper, but it simplifies some proofs.

Lemma 17: K is a simple algebraic extension of $\mathcal{K}$

Proof: It is sufficient to prove that $K = \mathcal{K}(\alpha, \beta)$ is a simple algebraic extension where α and β are algebraic over $\mathcal{K}$; i.e. that $\mathcal{K}(\alpha, \beta) = \mathcal{K}(\theta)$, some θ algebraic over $\mathcal{K}$. Then use induction.

Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_M$ be the distinct conjugates of α and β over $\mathcal{K}$ respectively; say $\alpha = \alpha_1$, $\beta = \beta_1$. Note that for $k \neq 1$, $\beta_k \neq \beta$. Therefore, for all i, and all $k \neq 1$, the equation

$$\alpha_i + x\beta_k = \alpha + x\beta$$

has at most one solution in $\mathcal{K}$. Since there are only a finite

number of such equations, choose an element c in $\mathcal{K}$, where c is not a solution; i.e.

$$\alpha_i + c\beta_k \neq \alpha + c\beta$$

$$\alpha_i \neq (\alpha + c\beta) - c\beta_k$$

for all $k \neq 1$, for all i. Let $\theta = (\alpha + c\beta)$, and show that $\mathcal{K}(\theta) = \mathcal{K}(\alpha, \beta)$. Certainly $\mathcal{K}(\theta) \subseteq \mathcal{K}(\alpha, \beta)$. It suffices to show that α and β are in $\mathcal{K}(\theta)$, because then $\mathcal{K}(\alpha, \beta) \subseteq \mathcal{K}(\theta)$. But if $\beta \in \mathcal{K}(\theta)$, then $\alpha = (\theta - c\beta) \in \mathcal{K}(\theta)$ also, so it will suffice to show that $\beta \in \mathcal{K}(\theta)$.

Let $f(x)$ and $g(x)$ be the minimal polynomials for α and β respectively over $\mathcal{K}$. $f(\theta - c\beta) = f(\alpha) = 0$, so β also satisfies $f(\theta - cx) = 0$. $g(x)$ and $f(\theta - cx)$ have only one root, β, in common for otherwise, $\alpha_i = \theta - c\beta_k$ for some $k \neq 1$ for some i, contrary to the choice of c.

$g(x)$ and $f(\theta - cx)$ are also polynomials over $\mathcal{K}(\theta)$, with the one root β in common. Let $h(x) \neq 0$ be the minimal polynomial for β over $\mathcal{K}(\theta)$. Then $h(x) \mid g(x)$ and $h(x) \mid f(\theta - cx)$ by the corollary to lemma 1. But this means that $h(x)$ is of degree at most 1, since $g(x)$ and $f(\theta - cx)$ have only one root in common: so $h(x) = \gamma x + \delta$, where $\gamma, \delta \in \mathcal{K}(\theta)$. Thus $\gamma\beta + \delta = 0$ or $\beta = -\delta/\gamma \in \mathcal{K}(\theta)$. qed

Lemma 18: If θ is algebraic over $\mathcal{K}$, then so is every element of $K = \mathcal{K}(\theta)$.

Proof: If θ is algebraic over $\mathcal{K}$ then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for $\mathcal{K}(\theta)$ as a vector space over $\mathcal{K}$, by lemma 16. Thus $\mathcal{K}(\theta)$ is a finitely generated vector space, and every element therein is algebraic over $\mathcal{K}$ by the remark following the definition of "algebraic."

qed

If the field E is a finite extension of the field F, and F is a finite extension of the field K, then E is a finite extension of K.[6] Consequently the degree over $\mathcal{K}$ of any element $\alpha \in K$ divides $n = [K : \mathcal{K}]$; for, let $F = \mathcal{K}(\alpha)$; then $\deg \alpha = [\mathcal{K}(\alpha) : \mathcal{K}] \mid [K : \mathcal{K}] = n$.

Lemma 19: If $\theta_1, \ldots, \theta_n$ are algebraic over $\mathcal{K}$, then so is every element of $\mathcal{K}(\theta_1, \ldots, \theta_n)$.

Proof: $\mathcal{K}(\theta_1)$ is a (simple) finite algebraic extension of $\mathcal{K}$ and $\mathcal{K}(\theta_1\theta_2)$ is a finite extension of $\mathcal{K}(\theta_1)$. The remarks above give that $\mathcal{K}(\theta_1,\theta_2)$ is finite over $\mathcal{K}$. Repeat the process and continue. Obtain $\mathcal{K}(\theta_1, \ldots, \theta_n)$ is finite over $\mathcal{K}$. So every element of $\mathcal{K}(\theta_1, \ldots, \theta_n)$ is algebraic over $\mathcal{K}$.

qed

Lemma 20: The totality of elements algebraic over forms a field.

Proof: Say α, β are algebraic over $\mathcal{K}$. It must be shown that $\alpha+\beta, \alpha-\beta, \alpha\beta, \alpha/\beta$, (where $\beta \neq 0$) are algebraic over $\mathcal{K}$. But the field $\mathcal{K}(\alpha,\beta)$ contains these 4 elements. The preceding corollary to lemma gives that the 4 elements are algebraic over $\mathcal{K}$.

qed

Note that the totality of elements algebraic over $\mathcal{K}$ is not a finite extension of $\mathcal{K}$. For suppose the field, call it T, were of degree n over $\mathcal{K}$. But the polynomial $(x^{n+1} - 2)$ is irreducible over T by Eisenstein's criterion; yet the algebraic number $2^{1/n+1}$, which satisfies $x^{n+1} - 2$, is of degree n+1 over T, a contradiction.

Note that $[\mathbb{Q}(\theta) : \mathbb{Q}]$ is the same as the degree of θ over $\mathbb{Q}$. Also note that every finite extension K of $\mathbb{Q}$ can be constructed by adjoining a single element θ, algebraic over $\mathbb{Q}$ i.e. $K = \mathbb{Q}(\theta)$.

Lemma 21: If α satisfies the equation

$$\alpha_n X^n + \ldots + \alpha_1 X + \alpha_0 = 0$$

where the α_i are algebraic over $\mathbb{Q}$, then α is algebraic over $\mathbb{Q}$. (Note this is not the same as lemma 14.)

Proof: Let $E = \mathbb{Q}(\alpha_0, \alpha_1, \ldots, \alpha_n)$ be a finite extension of $\mathbb{Q}$. α is algebraic over E, so $E(\alpha)$ is a finite extension of E. Thus $E(\alpha)$ is finite over $\mathbb{Q}$, and since $\alpha \in E(\alpha)$, α is algebraic over $\mathbb{Q}$.

qed

Definition: Let $K = \mathbb{Q}(\theta)$ be a finite extension of $\mathbb{Q}$ of degree n, and let $\alpha \in K$; let

$$\alpha = \sum_{i=0}^{n-1} c_i \theta^i = r(\theta)$$

(guaranteed by lemma 16); let $\theta_1, \ldots, \theta_n$ be the distinct conjugates of θ over $\mathbb{Q}$; then the elements

$$\alpha_i = r(\theta_i), \qquad i = 1, \ldots, n$$

are called the conjugates of α for $\mathbb{Q}(\theta)$.

Note that the conjugates of $\alpha\beta$ for $\mathbb{Q}(\theta)$ are $\alpha_1\beta_1, \alpha_2\beta_2, \ldots$ $\alpha_n\beta_n$ and the conjugates of $\alpha+\beta$ for $\mathbb{Q}(\theta)$ are $\alpha_1+\beta_1, \alpha_2+\beta_2, \ldots$ $\alpha_n+\beta_n$. The corollary to lemma [illegible] states that the degree of α over $\mathbb{Q}$ divides n. Let the degree of α be m.

Lemma 22: (i) The conjugates of α for $\mathbb{Q}(\theta)$ are the distinct

conjugates of α over $\mathcal{K}$ each repeated n/m times; (ii) $\alpha \in \mathcal{K}$ if and only if all conjugates of α for $\mathcal{K}(\theta)$ are the same; (iii) $\mathcal{K}(\alpha) = \mathcal{K}(\theta)$ if and only if all the conjugates of α for $\mathcal{K}(\theta)$ are distinct.

Proof: (i): Let

$$f(x) = \prod_{i=1}^{n} (x - r(\theta_i)),$$ where $\alpha = r(\theta)$.

Then f(x) is left unchanged by any permutation of the θ_i, so the same is true of the coefficients of f(x); consequently all the coefficients of f(x) are symmetric polynomials in the θ_i. Lemma 8 gives that the coefficients are in $\mathcal{K}$. Observe that $f(\alpha) = f(r(\theta)) = 0$. Let g(x) be the minimal polynomial for α over $\mathcal{K}$. Then $g(x) \mid f(x)$, and

$$f(x) = [g(x)]^s \cdot h(x)$$

where g(x) and h(x) are relatively prime. Show that h(x) is a constant, whence $h(x) = 1$, since both g(x) and f(x) are monic.

Suppose h(x) is not constant; then it must have some $r(\theta_i)$ as a root, i.e. $h(r(x)) = 0$ when x is one of the θ_i. Let p(x) be the minimal polynomial for θ, and hence, for all the θ_i. Then $p(x) \mid h(r(x))$, so all θ_i satisfy h(r(x)), in particular, θ does:

$$h(\alpha) = h(r(\theta)) = 0$$

But $g(\alpha) = 0$. This is impossible by corollary of lemma 2, whence $h(x) = 1$.

Thus $f(x) = [g(x)]^s$. The roots of f(x) are the conjugates of α for $\mathcal{K}$, and they are evidently the roots of g(x),

repeated s times. The roots of $g(x)$ are the distinct conjugates of α. The degree of $f(x)$ is n, and the degree of $g(x)$ is m. Thus $s = n/m$.

(ii): If $\alpha \in \mathbb{K}$, then $g(x) = x - \alpha$, $m = 1$, $s = n$, $f(x) = [g(x)]^n = (x - \alpha)^n$. Conversely, if all the conjugates are the same, then $f(x) = (x - \alpha)^n$, $s = n$, $m = 1$, $g(x) = x - \beta = 0$, where $\beta \in \mathbb{K}$, so $\alpha = \beta \in \mathbb{K}$

(iii): Since $n = s \cdot m$, or

$$[\mathbb{K}(\theta):\mathbb{K}] = [\mathbb{K}(\theta):\mathbb{K}(\alpha)] \cdot [\mathbb{K}(\alpha):\mathbb{K}],$$

then $\mathbb{K}(\theta) = \mathbb{K}(\alpha)$ if and only if $s = 1$. $s = 1$ implies that $f(x) = g(x)$, so the conjugates of α are the distinct conjugates. If the conjugates are distinct, then $s = 1$.

qed

Definition: $f(x)$ in the above lemma is called the field polynomial for α over $\mathbb{K}(\theta)$.

Definition: Suppose $\mathbb{K} = \mathbb{K}(\theta)$ is of degree $= n$ over $\mathbb{K}$, and $\alpha_1, \ldots, \alpha_n$ is a basis; let the conjugates of α_j for K be denoted by $\alpha_j^{(1)}, \alpha_j^{(2)}, \ldots \alpha_j^{(n)}$; then the discriminant of the set $\alpha_1, \ldots, \alpha_n$ is defined by

$$\triangle[\alpha_1, \ldots, \alpha_n] = \left| \alpha_j^{(i)} \right|^2,$$

where $\left|a_j^{(i)}\right|$ is the determinant

$$\begin{vmatrix} a_1^{(1)} & a_2^{(1)} & \cdots & a_n^{(1)} \\ a_1^{(2)} & a_2^{(2)} & \cdots & a_n^{(2)} \\ \vdots & \vdots & & \vdots \\ a_1^{(n)} & a_2^{(n)} & \cdots & a_n^{(n)} \end{vmatrix}.$$

Lemma 23: Suppose $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are two bases for $K=\mathbb{Q}(\Theta)$ as a vector space over $\mathbb{Q}$, where $\beta_k = \sum_{j=1}^{n} c_{jk}\alpha_j$, $k=1,\ldots,n$. Then

$$\Delta[\beta_1, \ldots, \beta_n] = |c_{jk}|^2 \cdot \Delta[\alpha_1, \ldots, \alpha_n].$$

Proof: It suffices to show that

$$\begin{pmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \cdots & \beta_1^{(n)} \\ \beta_2^{(1)} & \beta_2^{(2)} & \cdots & \beta_2^{(n)} \\ \vdots & \vdots & & \vdots \\ \beta_n^{(1)} & \beta_n^{(2)} & \cdots & \beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{21} & \cdots & c_{n1} \\ c_{12} & c_{22} & \cdots & c_{n2} \\ \vdots & \vdots & & \vdots \\ c_{1n} & c_{2n} & \cdots & c_{nn} \end{pmatrix} \cdot \begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_n^{(1)} \\ \alpha_2^{(1)} & \alpha_2^{(2)} & \cdots & \alpha_n^{(2)} \\ \vdots & \vdots & & \vdots \\ \alpha_n^{(1)} & \alpha_n^{(2)} & \cdots & \alpha_n^{(n)} \end{pmatrix},$$

since the determinant of a matrix is the same as that of its transpose.

Consider any transformation on $K=\mathbb{Q}(\Theta)$, $\sigma_i: K \longrightarrow \mathbb{Q}$ defined for all $\gamma \in K$ by

$$\sigma_i(\gamma) = \gamma^{(i)}.$$

(Since all the conjugates of elements of K might not lie in K, σ_i might not be an automorphism of K.) Since each element has only one i^{th} conjugate, and by the remark immediately following the definition of "conjugate", σ_i is a homomorphism of K. Since K is a field and σ_i is not the 0-map, σ_i is an isomorphism.

Now it is given that $\beta_k = c_{1k}\alpha_1 + \ldots + c_{nk}\alpha_n$. Operate on this equation with σ_i: $\sigma_i(\beta_k) = \sigma_i(c_{1k}\alpha_1 + \ldots + c_{nk}\alpha_n)$

$$\beta_k^{(i)} = (c_{1k}\alpha_1 + \ldots + c_{nk}\alpha_n)^{(i)}$$

$$= c_{1k}\alpha_1^{(i)} + \ldots + c_{nk}\alpha_n^{(i)}$$

since σ_i is an isomorphism, and since for $c_{jk} \in \mathbb{Q}$, $c_{jk}^{(i)} = c_{jk}$ (lemma 22, (ii)). This gives the lemma.

qed

Corollary: If $K = \mathbb{Q}(\theta)$ and $\alpha, \beta, \gamma, \delta \in K$ and for all $x \in K$, the i^{th} conjugate of x is $x^{(i)}$, then

$$(\alpha\beta + \gamma\delta)^{(i)} = \alpha^{(i)}\beta^{(i)} + \gamma^{(i)}\delta^{(i)}$$

Proof: σ_i, in the lemma, is an isomorphism; the corollary follows.

qed

Lemma 24: The discriminant of any basis for $\mathbb{Q}(\theta)$ is in $\mathbb{Q}$, and is never 0. If θ and the conjugates of θ are real, then the discriminant of any basis is positive.

Proof: If $\mathbb{Q}(\theta)$ is of degree n over $\mathbb{Q}$, by lemma 16, a particular basis for $\mathbb{Q}(\theta)$ is $\{1, (\theta), \ldots, (\theta)^{n-1}\}$ It follows from the preceding corollary that for this basis

$$(\theta^i)^{(j)} = (\theta^{(j)})^i.$$

Therefore

$$D(\theta) = \Delta[1, \theta, \ldots, \theta^{n-1}]$$

$$= \begin{vmatrix} 1 & \theta^{(1)} & \cdots & (\theta^{(1)})^{n-1} \\ 1 & \theta^{(2)} & \cdots & (\theta^{(2)})^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \theta^{(n)} & \cdots & (\theta^{(n)})^{n-1} \end{vmatrix}^2$$

This Vandermonde determinate is known[7] to have the value

$$D(\theta) = \prod_{i<j} (\theta^{(j)} - \theta^{(i)})^2$$

Thus $D(\theta) \neq 0$, since the conjugates of (θ) for $\mathbb{Q}(\theta)$ are distinct. Since interchanging any two rows of a matrix does not alter its determinate, $D(\theta)$ is symmetric in the $(\theta^{(i)})$.

Then lemma 8 gives that $D(\theta) \in \mathcal{O}$.

If all the $(\theta)^{(i)}$ are real, $D(\theta)$ is positive, because every factor is squared.

qed

Lemma 25: If $\alpha_1, \ldots, \alpha_n$ is any basis of K consisting only of (algebraic) integers, then $\Delta[\alpha_1, \ldots, \alpha_n]$ is a rational integer.

Proof: If all the conjugates of $\alpha_1, \ldots, \alpha_n$ are not in K, adjoin them to K to get a K-extension, $L = K(\alpha_1^{(1)}, \alpha_1^{(2)}, \ldots, \alpha_1^{(j)}, \ldots, \alpha_n^{(n-1)}, \alpha_n^{(n)})$. L is finite over K and hence over $\mathcal{O}$. Then since each of these conjugates satisfies its minimal polynomial with coefficients in $\mathcal{Z}$, they are all in Z_L. Since Z_L is a ring, the discriminant

$$\Delta = \Delta[\alpha_1, \ldots, \alpha_n] = \begin{vmatrix} \alpha_1^{(1)} & \alpha_2^{(1)} & \cdots & \alpha_n^{(1)} \\ \alpha_1^{(2)} & \alpha_2^{(2)} & \cdots & \alpha_n^{(2)} \\ \vdots & \vdots & & \vdots \\ \alpha_1^{(n)} & \alpha_2^{(n)} & \cdots & \alpha_n^{(n)} \end{vmatrix}^2$$

is in Z_L. Lemma 8 gives that $\Delta \in \mathcal{O}$. So by lemma 17, $\Delta \in Z_L \cap \mathcal{O} = \mathcal{Z}$.

qed

Lemma 26: K has an integral basis.

Proof: $K = \mathcal{O}(\theta)$ for some θ algebraic over $\mathcal{O}$. Consider all bases for K that consist entirely of integers ($1, \theta, \ldots, \theta^{n-1}$ is such a basis). By lemma 25, the discriminants of such bases are in $\mathcal{Z}$. Therefore choose one, $\{\omega_1, \ldots, \omega_n\}$, where $|\Delta(\omega_1, \ldots, \omega_n)| = d$ is a minimum. By lemma 24, $d \neq 0$. Show that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for K.

Suppose that it is not. Then there exists an integer

$\omega \in Z_K$ such that

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n$$

where the a_i are all rational but not all rational integral (this is possible since $\{\omega_1, \ldots, \omega_n\}$ is at any rate a basis for K.) Say that a_1 is not a rational integer. Then $a_1 = b + r$, $r \in \mathbb{Q}$, b is a rational integer, and $0 < r < 1$. Define

$$\begin{aligned}
\omega_1' &= (a_1 - b)\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \\
&= \omega - b\omega_1 \\
\omega_2' &= \omega_2 \\
&\vdots \\
\omega_n' &= \omega_n
\end{aligned}$$

If

$$A = \begin{pmatrix} a_1 - b & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

then $[\omega_1', \ldots, \omega_n'] = A[\omega_1, \ldots, \omega_n]$ Since $\det A = (a_1 - b) = r \neq 0$, $\{\omega_1', \ldots, \omega_n'\}$ is a basis for K, and A is the matrix of the change of basis. Moreover $\{\omega_1, \ldots, \omega_n'\}$ consists entirely of integers.

By lemma 23 then

$$\Delta[\omega_1', \ldots, \omega_n'] = r^2\Delta[\omega_1, \ldots, \omega_n]$$

$$|\Delta[\omega_1', \ldots, \omega_n']| < |\Delta[\omega_1, \ldots, \omega_n]| .$$

This contradicts the minimality of d; so $\{\omega_1, \ldots, \omega_n\}$ is an integral basis

qed

Thus Z_K is a finitely generated $\mathbb{Z}$-module.

Lemma 27: Z_K is Noetherian.

Proof: Lemma 9 gives that ACC holds for sub-$\mathbb{Z}$-modules of Z_K. Any ideal of Z_K is a sub-$\mathbb{Z}$-module of Z_K, and so is finitely generated over $\mathbb{Z}$; i.e. if A is an ideal of Z_K then there exist elements $\alpha_1, \ldots, \alpha_n$ in Z_K such that every element β in A can be represented as

$$\beta = z_1\alpha_1 + \ldots + z_n\alpha_n$$

where the $z_i \in \mathbb{Z}$. But the z_i are also in Z_K; thus the ideal A is generated by the elements $\alpha_1, \ldots, \alpha_n$ and the lemma is proved.

qed

IV

The third condition that Z_K satisfies is that its prime ideal and maximal ideals are in fact the same. This is now demonstrated. First it is shown that every element of Z_K can be factored into a product of prime elements (not necessarily uniquely).

Definition: Let A be an ideal of a ring R and $A \neq (0)$, $A \neq R$; then A is a prime ideal of R if for all $\alpha, \beta \in R$ such that $\alpha \cdot \beta \in R$, either $\alpha \in R$ or $\beta \in R$.

Definition: In a ring R, if $\alpha, \beta \in R$, α divides β ($\alpha \mid \beta$) if $\beta/\alpha \in R$; μ is a unit if $\mu \mid 1$; α is a prime element if α is not 0 or a unit, and if any factorization $\alpha = \beta\gamma$ into integers implies either β or γ is a unit. "Prime element" is often abbreviated to "prime."

Definition: If α is an integer in K, and $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ are the n conjugates of α, then the norm of α, denoted by $N(\alpha)$, is $N(\alpha) = \alpha_1 \alpha_2 \cdots \alpha_n$.

Lemma 28: $N(\alpha)$ is a rational integer.

Proof: Let $f(x)$ be the field polynomial for α. Since $f(x)$ is a power of the minimal polynomial, $f(x)$ has coefficients in Z. Thus

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$
$$= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n);$$

where a_0 is in Z. Observe that

$$a_0 = (-1)^n \alpha_1 \cdots \alpha_n$$
$$\alpha_1 \cdots \alpha_n = (-1)^n a_0 \in Z.$$

qed

Lemma 29: $N(\alpha\beta) = N(\alpha)\cdot N(\beta)$.

Proof: If $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are the conjugates of α and β respectively, then the conjugates of $\alpha\beta$ are $\alpha_1\beta_1, \ldots, \alpha_n\beta_n$. This gives the lemma.

qed

Lemma 30: α is a unit in K if and only if $N(\alpha) = \pm 1$.

Proof: α is a unit if and only if $\alpha \mid 1$. If $\alpha \mid 1$, then $N(\alpha) \mid N(1) = 1$, so $N(\alpha) = \pm 1$. If $N(\alpha) = \pm 1$, then $\alpha_1 \cdots \alpha_n \mid 1$ so $\alpha_1 = \alpha \mid 1$.

qed

Lemma 31: If $N(\alpha)$ is prime in $\mathbb{Z}$, then α is prime in K.

Proof: If $\alpha = \beta\gamma$, then $N(\alpha) = N(\beta)\cdot N(\gamma)$, so either $N(\beta)$ or $N(\gamma)$ is ± 1, since $N(\alpha)$ is prime. This means that either β or γ is a unit in K.

qed

Lemma 32: Every element of Z_K, not 0 or a unit can be factored into a product of primes (not necessarily uniquely).

Proof: Suppose the lemma is false, and $\alpha \in Z_K$, α is not a prime, a unit, or a finite product of primes. Then $\alpha = \beta\gamma$, where β (or γ) has the same property. Thus $\beta = \beta'\gamma'$ where β' (or γ') has the same property. $\beta' = \beta''\gamma''$ etc. Thus an ascending chain of ideals is constructed:

$$(\alpha) \subseteq (\beta) \subseteq (\beta') \subseteq \cdots$$

The inclusions are proper, because none of $\{\alpha, \beta, \beta', \ldots\}$ are associated, by their construction. So here is a neverending strictly ascending chain, which is impossible, and the lemma is true.

qed

The product of two ideals A and B in a ring R is usually defined to be the smallest ideal containing all products $\alpha\beta$ where $\alpha \in A$, $\beta \in B$. It follows immediately that if $A = \{\alpha_1, \ldots, \alpha_n\}$, $B = \{\beta_1, \ldots, \beta_n\}$, then $AB = \{\alpha_1\beta_1, \ldots \alpha_i\beta_j, \ldots \alpha_n\beta_m\}$ for all i, j.

Definition: For ideals A and B in Z_K, A is a factor of B (written $A|B$), if an ideal C of Z_K exists such that $B = A \cdot C$. A is called a divisor of B if $A \supseteq B$.

Note the distinction between a factor and a divisor. It follows from the definition that a factor is a divisor. It will be shown shortly that a divisor is a factor.

Lemma 33: An ideal P of Z_K different from (0) or $(1)_\Lambda = Z_K$ is maximal if and only if it is prime.

Proof: It is well-known that all maximal ideals are prime. Therefore it suffices to show that a prime ideal P is maximal.

Let $P = (\alpha_1, \ldots, \alpha_s) \subseteq P'$, $P \neq P'$. Show that $P' = (1)$. Let $\alpha \in P'$, $\alpha \notin P$. Then all powers α^j of α are in P'.

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for K. Let $\beta \in P$. Then $\pm N(\beta) \in P$, so P contains a positive rational integer c. Every integer in K can be written in the form

$$\delta = \sum_{i=1}^{n} d_i \omega_i$$

where the $d_i \in Z$. Each d_i can be written

$$d_i = q_i c + r_i,$$

where $q_i, r_i \in Z$, $0 \leq r_i \leq c$, $1 \leq i \leq n$. Thus for all i, r_i can only assume c different values. Therefore

$q_i c$

$$\begin{aligned}\delta &= \sum_{i=1}^{n} (q_i c + r_i)\omega_i \\ &= c\left(\sum_{i=1}^{n} q_i \omega_i\right) + \sum_{i=1}^{n} r_i \omega_i \\ &= c\gamma + \sum_{i=1}^{n} r_i \omega_i ,\end{aligned}$$

where $\gamma \in Z_K$.
In particular

$$\alpha^j = c\gamma_j + \sum_{i=1}^{n} r_{ij}\omega_i .$$

Thus, for all powers α^j of α, $\alpha^j - c\gamma_j$ can only assume a finite number of different values. This means there exist two rational integers k and h, $k > h$, such that

$$\alpha^k - c\gamma_k = \alpha^h - c\gamma_h .$$

$\alpha^k - \alpha^h = c(\gamma_k - \gamma_h)$ is in P, since c is in P. Therefore $\alpha^h(\alpha^{k-h} - 1)$ is in P, which means either α^h or $\alpha^{k-h} - 1$ is in P since P is prime. But α^h could not be in P because then $\alpha \in P$ (since P is prime), contradicting the choice of α. Thus $\alpha^{k-h} - 1 \in P \subseteq P'$. But all powers of α, and in particular α^{k-h} are in P'. So $\alpha^{k-h} - (\alpha^{k-h} - 1) = 1 \in P'$ and $P' = (1)$. This means P is maximal.

qed

From this lemma it is seen that the terms "prime ideal" and maximal ideal" are interchangeable in Z_K.

The three conditions have now been established. Before getting to the main theorem however, one more lemma must be proved,

Definition: ACC is valid in an R-module, if every ascending chain of sub-modules $M_1 \subseteq M_2 \subseteq \ldots$ is finite in length.

It is well-known[8] that the following are equivalent:

(i) ACC is valid in an R-module M, and (ii) every sub-module of M has a finite basis.

Lemma 34: Let R be a Noetherian ring; integrally closed in its fraction field S, and $b \in S$; then $b \in R$ if and only if all powers b^h of b may be represented by fractions of S with the same denominator c from R.

Proof: Suppose all powers b^h of b are expressible as a fraction with the same denominator c; then

$$b^h = (r_{bh_1}/c) + \ldots + (r_{bh_n}/c)$$

$$= (r_{bh_1} \cdot c^{-1}) + r_{mb_h} \cdot c^{-1}$$

for all h, with r_{bh_i} and c elements of R. Then $c^{-1} \in S$, so that all powers of b are in the finitely generated R-module (c^{-1}). By lemma 10, b is integral over R. Since R is integrally closed in S, then $b \in R$.

Conversely if $b \in R$, then all powers b^h of b are in the ring R; thus $b^h = b^h/1$, for all h.

qed

V

Theorem: (Dedekind) Let the ring R satisfy the following three properties: (i) R is Noetherian, (ii) prime ideals and maximal ideals are the same; (iii) R is integrally closed in its quotient field S; then every ideal of R, not (0) or R, can be represented uniquely (except for order) as a product $P_1 P_2 \ldots P_n$ of prime ideals of R.

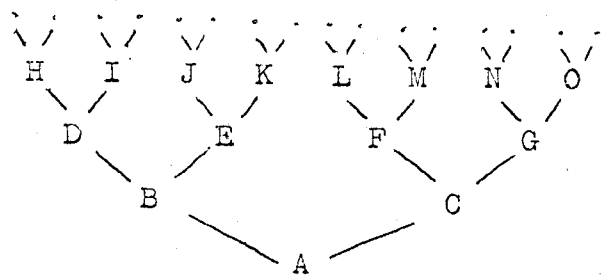
The proof requires more lemmas. Throughout assume the three conditions of the theorem hold for the ring R.

Lemma 35: For every ideal A of R there exist prime ideals $P_1, \ldots, P_n$ of R such that $A \subseteq P_i$ for all i, and

$$P_1 P_2 \cdots P_n \subseteq A.$$

Proof: Suppose $A = (\alpha_1, \ldots, \alpha_r)$. If A is a prime ideal, the lemma is true; if not then there exist $\beta, \gamma \in R$ such that $\beta \cdot \gamma \in A$, yet $\beta, \gamma \notin A$.

Let $B = (\alpha_1, \ldots, \alpha_r, \beta)$ and $C = (\alpha_1, \ldots, \alpha_r, \gamma)$. Then $A \subsetneq B$, $A \subsetneq C$, and $BC \subseteq A$. If B and C are prime, the lemma is true; if either (or both) of B and C is not prime, repeat the process with the one, say B, (or both) that is not prime, obtaining two ideal divisors D, E of B such that B divides their product $D \cdot E$. (Do the same with C if C is not prime). If D and/or E is not prime, repeat the process and continue. Note that at each stage, the new ideals obtained divide A (e.g. $D \supseteq B \supseteq A$ and $E \supseteq B \supseteq A$). Thus a series of ascending chains is formed



But R is Noetherian, so all the ascending chains must stop after a finite number of stages. This means that at the final stages all the ideals are maximal, and hence prime. Each one divides A, yet their product is in A. This gives the lemma.

qed

Lemma 36: If P is a prime ideal in R, and A,B are two ideals such that $AB \subseteq P$, yet $A \not\subseteq P$, then $B \subseteq P$.

Proof: Say $B \not\subseteq P$. Then there exist $\alpha \in A$, $\beta \in B$ such that $\alpha,\beta \notin P$. But $\alpha\cdot\beta \in P$. This is impossible. qed

Definition: If $A \neq (0)$ is an ideal in R and S is the quotient field of R, designate by A^{-1} the totality of elements $\beta \in S$, where $\beta\pi \in R$ for all $\pi \in A$; β need not be in R.

Lemma 37: Let P be a prime ideal in R; then P^{-1} contains an element not in R.

Proof: Let $c \neq 0 \in P$. By lemma 35, there is a finite product of primes $P_1 \cdots P_r$ such that $P_1 \cdots P_r \subseteq (c)$. Assume this product is irredundant, i.e. there is no shorter product of P_i in (c). Since $(c) \subseteq P$, $P_1 \cdots P_r \subseteq P$, then one of the $P_i \subseteq P$ by the preceding lemma. Say $P_1 \subseteq P$. But since $P \neq R$, and P_1 is maximal, $P_1 = P$. Thus

$$PP_2 \cdots P_r \subseteq (c).$$

$P_2 \cdots P_r \not\subseteq (c)$, so there is $b \in P_2 \cdots P_r$ such that $b \notin (c)$. $bP \subseteq PP_2 \cdots P_r \subseteq (c)$, so $bP \subseteq (c)$; i.e. for all $\pi \in P$, $b\pi \in (c) \subseteq R$. Thus $c \mid b\pi$, or $\pi(b/c) \in R$, for all $\pi \in P$. This means $(b/c) \in P^{-1}$.

But notice that $b,c \in R$, yet $b \notin (c)$. Thus $c \nmid b$ in R; i.e. $b/c \notin R$. (b/c) then is the required element.

qed

Definition: Let R be an integral domain, $R \subseteq S$, its quotient field; if $M \subseteq S$ is a finitely generated R-module, where the module product is defined as the ordinary product in S, then M is called a fractional ideal of R.

Note that M is a fractional ideal of R, and $M \subseteq R$ if and only if M is an ideal of R.

Lemma 38: Let R be a Noetherian ring, $R \subseteq S$, its quotient field; let H be a non-empty subset of S; then H is a fractional ideal of R if and only if there exists an element $b \in S$ such that bH is an ideal in R.

Proof: If H is a fractional ideal, then

$$H = R\frac{r_1}{s_1} + \ldots + R\frac{r_n}{s_n},$$

for some generators $\frac{r_1}{s_1}, \ldots, \frac{r_n}{s_n}$ in S. Let $b = s_1 \ldots s_n$. Then

$$bH = (Rr_1 s_2 \ldots s_N) + (Rs_1 r_2 \ldots s_N) + \ldots + (Rs_1 s_2 \ldots r_N)$$
$$= (r_1 s_2 \ldots s_N, s_1 r_2 \ldots s_N, \ldots, s_1 s_2 \ldots r_N)$$

where the r_i and $s_i \in R$. So bH is an ideal in R.

Conversely if $b \in S$, and bH is an ideal of R, then $bH = Rr_1 + \ldots + Rr_n$, for some $r_i \in R$. Therefore

$$H = R.\frac{r_1}{b} + \ldots + R.\frac{r_n}{b},$$

and H is a finitely generated R module in S.

qed

Lemma 39: If R is a Noetherian ring, $R \subseteq S$, the quotient field of R, and A is a non-zero ideal of R, then A^{-1} is a fractional ideal of R.

Proof: $R \subseteq A^{-1}$, so A^{-1} is not empty. If $a, b \in A$, then $a - b \in A^{-1}$, and if $r \in R$, then $ra \in A^{-1}$. Thus A^{-1} is a module over R.

Let $d \in A$, $d \neq 0$, and let

$$B = \{da \mid a \in A^{-1}\}.$$

Then B is non-empty and $B \subseteq R$ by definition of A^{-1}. If $b_1, b_2 \in B$, then $b_1 = da_1$, $b_2 = da_2$ and $b_1 - b_2 = d(a_1 - a_2) \in B$, for $a_i \in A^{-1}$. If $r \in R$, then $rb_1 = d(ra_1) \in B$. Thus B is an ideal of R. But $A^{-1} = (1/d)B$, and $1/d \in S$. So lemma 38 gives that A^{-1} is a fractional ideal.

qed

Definition: If R, S are rings, $R \subseteq S$, and if U, V are two R modules in S, then the ~~ideal~~ module product $U \cdot V$ is defined as the smallest module in S containing all products $u \cdot v$, where $u \in U$ and $v \in V$; i.e. $U \cdot V$ is all finite sums of products of the form $u \cdot v$.

Thus if $U = (\alpha_1, \ldots, \alpha_n)$, $V = (\beta_1, \ldots, \beta_m)$ are finitely generated R-modules in S, then $U \cdot V = (\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_n\beta_m)$, where $1 \leq i \leq n$, $1 \leq j \leq m$. Note this definition is consistent with the definition for the product of ideals (an ideal being a special module).

Lemma 40: If P is a prime ideal in R, and S is the quotient field of R, then $P \cdot P^{-1} = R$.

Proof: $R \subseteq P^{-1}$, so $P = R \cdot P \subseteq P^{-1}P$. PP^{-1} is an ideal of R, since it is in R, and it is an R-module, so since P is maximal, $PP^{-1} = P$ or $PP^{-1} = R$. Show that $PP^{-1} = P$ is impossible.

Suppose $PP^{-1} = P$. Then $P(P^{-1})^2 = (PP^{-1})P^{-1} = P$, $P(P^{-1})^3 = P$, ... Say $a \neq 0 \in P$, $b \in P^{-1}$. Then $ab^h \in P(P^{-1})^h = P$, for all powers b^h of b. So $c_h = ab^h \in R$. Thus every power b^h of b can be represented as a fraction c_h/a with the same denominator a. Lemma 34 gives $b \in R$. This is true for

all $b \in P^{-1}$, contradicting lemma 37.

Thus $PP^{-1} = P$ is impossible, and $PP^{-1} = R$.

qed

Lemma 41: Every ideal A in R, where $A \neq (0)$, $A \neq R$, is a product of prime ideals.

Proof: Let S be the quotient field of R. Suppose $A \neq R$, $A \neq (0)$. By lemma 35, there are prime ideas $P_1, \ldots, P_r$ such that their product is in A, yet $P_i \supseteq A$, for all i. Again choose r as small as possible. Let P be an arbitrary prime ideal containing A (the existence of P is guaranteed by lemma 35. Thus $P_1 \ldots P_r \subseteq P$, and lemma 36 gives that for some i, $P_i \subseteq P$. Hence $P_i = P$ since P_i is maximal. Say $P_1 = P$. Then

$$PP_2 \ldots P_r \subseteq A$$
$$P^{-1}PP_2 \ldots P_r \subseteq P^{-1}A$$
$$P_2 \ldots P_r \subseteq P^{-1}A$$

AP^{-1} is an ideal in R, since $PP^{-1} \subseteq R$ and $A \subseteq P$; thus it is an R-module because it is the product of two R-modules in S; an R-module in R is an ideal of R. So AP^{-1} is an ideal in R containing a product of less than r prime ideals. Now use induction on r, and assume the lemma is valid for all ideals of R containing a product of fewer than r prime ideals. Note that the lemma is true for ideals containing exactly one prime (maximal)ideal. Thus the lemma holds for AP^{-1}:

$$AP^{-1} = P_2' \ldots P_m'.$$

So $A = AP^{-1}P = PP_2' \ldots P_m'$.

qed

Lemma 47: Suppose A, B are ideals in R, where $A \subseteq B$; say $A = P_1 \dots P_r$, $B = P_1' \dots P_s'$, where the ideals P_i and P_i' are prime; then every prime ideal that occurs in the representation of B occurs in the representation of A, and at least as often.

Proof: $P_1' \supseteq B \supseteq A$, so P_1' includes one of the P_i, say P_1, and so $= P_1$ as before: $P_1' = P_1$. But $A \subseteq B$, so

$$P_1^{-1}A \subseteq P_1^{-1}B$$

$$P_1^{-1}A = P_2 \dots P_r$$

$$P_1^{-1}B = P_2' \dots P_s' .$$

Using induction on s, assume the theorem is true for any ideal represented by a product of t prime ideals, where $t < s$. (Note that the lemma is true for $s = 0$; then $B = R$.) Thus each of the ideals P_2', ..., P_s' occurs among the P_2, ..., P_r at least as often as among the P_2', ..., P_s'. The lemma follows immediately.

qed

Corollary 1: The theorem.

Proof: Let $A = B$ in the preceding lemma.

qed

Corollary 2: A divisor is a factor.

Proof: If $A \subseteq B$, then $A = BC$, where C is the product of those prime ideals of A left over, when those of B are stricken.

Corollary 3: Any ideal in Z_K can be represented as a product of prime ideals, unique except for order.

VI

There are a few interesting applications of this theorem that follow quite readily. For completeness it should be noted that the converse, together with a slightly more stringent condition, is also true.

Lemma 43: Let R be an integral domain, where every non-trivial ideal can be represented uniquely as a product of prime ideals; furthermore suppose for ideals, if $A \subseteq B$, then $A = B \cdot C$ for some ideal C; then (i) R is Noetherian, (ii) prime ideals are maximal, and (iii) R is integrally closed in its quotient field S.

Proof: (i) follows directly since every ideal $A = P_1^{s_1} \cdots P_n^{s_n}$ has only finitely many divisors $P_1^{r_1} \cdots P_n^{r_n}$, where $r_i \leq s_i$. In particular a prime ideal P has only P and R as divisors, implying that P is maximal; so (ii) is satisfied.

For (iii), let $\lambda \in S$ and λ be integral over R of degree $m \neq 0$. Then by the definition, λ^m is expressible linearly in terms of $\lambda^0, \lambda', \ldots, \lambda^{m-1}$. i.e. λ^m is in the R-module $L = (\lambda^0, \lambda', \ldots, \lambda^{m-1})$. If $\lambda = a/b$, where $a, b \in R$, L may be transformed into an ideal of R by multiplying by the ideal $B = (b^{m-1})$. Note that $L^2 = L$. Then

$$(LB)(LB) = L^2B^2 = LB^2 = (LB)B,$$

and the uniqueness implies

$$LB = B.$$

Multiply both sides by the R-module $(b^{-(m-1)})$, obtaining $L = R$. Then $\lambda \in L \subseteq R$, and (iii) is satisfied. q.e.d.

Representations as products of primes of the two ideals $A \cap B$ and $A + B$ in Z_K are quite simple due to the theorem.

Definition: If $A = P_1^{h_1} \ldots P_r^{h_r}$, $B = P_1^{k_1} \ldots P_r^{k_r}$, are two arbitrary ideals in Z_K (h_i, k_i may $= 0$, in which case $P_i^{h_i}$ or $P_i^{k_i}$ is defined as $P_i^{0} = (1) = Z_K$); then the greatest common divisor (A,B), of A and B is

$$(A,B) = P_1^{n_1} \ldots P_r^{n_r}$$

where $n_i = \min(h_i, k_i)$; the least common multiple, $[A, B]$, is

$$[A, B] = P_1^{m_1} \ldots P_r^{m_r} \quad ,$$

where $m_i = \max(h_i, k_i)$.

The greatest common divisor is abbreviated GCD; the least common multiple is abbreviated LCM. Note that D is the GCD of A and B if and only if $D|A$, $D|B$, and for every other divisor E of A and B, $E|D$. Similarly, M is the LCM of A and B if and only if $A|M$, $B|M$, and for every other multiple F of A and B, $M|F$ (U is a multiple of V if $V|U$).

Lemma 44: If A and B are ideals in Z_K, then $A + B = (A,B)$ and $A \cap B = [A,B]$.

Proof: Clearly $A + B \supseteq A$ and $A + B \supseteq B$, so by corollary 2 of lemma 42, $(A + B)|A$ and $(A + B)|B$. Further if $E|A$ and $E|B$, then $E \supseteq A$ and $E \supseteq B$, so $E \supseteq A + B$ and $E|(A + B)$. So $A + B = (A,B)$, the GCD.

On the other hand note that both A and B contain $A \cap B$ so $A|A \cap B$ and $B|A \cap B$. Further, if $A|E$ and $B|E$, then both A and B include E, so $A \cap B \supseteq E$; this implies $A \cap B|E$. So $A \cap B$ is the LCM: $[A,B]$.

qed

Notice that if $A = (\alpha_1, \ldots, \alpha_n)$ and $B = (\beta_1, \ldots, \beta_m)$ then

$$A + B = (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$$
$$A \cap B = (\gamma_1, \ldots, \gamma_k),$$

where the γ_i are those elements of Z_K that are generators of both A and B. Thus, using the above lemma, the exact generators of both the GCD and LCM of A and B can be found.

The following lemma verifies any speculation that the set of fractional ideals of Z_K might be a group.

Lemma 45: The non-zero fractional ideals of Z_K form an abelian group under the operation of the product of modules.

Proof: Certainly the product of two fractional ideals is a fractional ideal. The identity is $Z_K = (1)$. Given an ideal $A = P_1 P_2 \ldots P_n$, let $A^{-1} = P_1^{-1} P_2^{-1} \ldots P_n^{-1}$. Certainly A^{-1} is a fractional ideal, and lemma 40 gives that $A \cdot A^{-1} = Z_K = (1)$. Commutativity and associativity hold in the group since they hold in K.

qed

It is known that every ideal in Z_K is finitely-generated. The following lemma shows that every ideal is in fact generated by at most two elements.

Lemma 46: If A and D are ideals in Z_K, $A \neq (0)$ and $D \neq (0)$, and $A \subseteq D$, then there is an element $d \in D$ such that the GCD $(A,(d)) = D$.

Proof: Let $A = P_1^{h_1} \ldots P_r^{h_r}$, $D = P_1^{k_1} \ldots P_r^{k_r}$, where $0 \leq k_i \leq h_i$. d must be chosen so that $D \mid (d)$, but (d) has no further divisors in common with A, (i.e. so that

$$(d) = P_1^{k_1} \ldots P_r^{k_r} \cdot B = D \cdot B$$

for some ideal $B \subseteq D$ where $(A,B) = (1)$. Let

$$C = P_1^{k_1+1} \cdots P_r^{k_r+1} ,$$

and

$$C_i = P_1^{k_1+1} \cdots P_i^{k_i} \cdots P_r^{k_r+1}$$

$$= C \cdot P_i^{-1} .$$

Then $C \subseteq C_i \subseteq D$, so for all i, there is an element $d_i \in C_i$, but $d_i \notin C$. Thus $C_i \mid (d_i)$, so $P_j^{k_j+1} \mid (d_i)$ and $d_i \in P_j^{k_j+1}$ for $j \neq i$; also $P_i^{k_i+1} \nmid (d_i)$, so $d_i \notin P_i^{k_i+1}$. The sum

$$d = d_1 + \cdots + d_r \in D$$

since $d_i \in D$ for all i; thus D is a factor of (d). But (d) has no further in common with A, since

$$d_i \notin P_i^{k_i+1}$$

and

$$d \notin P_i^{k_i+1}$$

so $P_i^{k_i+1}$ is not a factor of (d); but if A had a further factor in common with (d), $P_i^{k_i+1}$ would be a factor of (d). Thus the greatest common factor, or GCD, of A and (d) is D.

qed

Corollary: Every ideal D in Z_K is generated by at most two elements, (a, d), where a may be picked arbitrarily in D.

Proof: In the lemma let A be (a), where a is picked arbitrarily in D. Then D is the GCD of (a) and (d); $D = ((a),(d)) = (a, d)$.

qed

It has been shown that Z_K is in general, not a UFD. However, Z_K is a UFD on occasion, and it will now be shown

that in this case Z_K is a principal ideal domain (PID). Preliminary lemmas are required.

Lemma 47: If

$$f(x) = \delta_m x^m + \ldots + \delta_1 x + \delta_0$$

is in $Z_K[x]$, $\delta_m \neq 0$, and π is one of its roots, then every coefficient of $f(x)/(x - \pi)$ has coefficients in Z_K (π may or may not be in Z_K).

Proof: $\delta_m \pi \in Z_K$ by lemma 14, because it satisfies the equation

$$g(x) = x^m + \delta_{m-1} x^{m-1} + \delta_{m-2}\delta_m x^{m-2} + \ldots$$
$$\ldots + \delta_1 \delta_m{}^{m-2} x + \delta_0 \delta_m{}^{m-1} = 0$$

$(g(\delta_m \pi) = \delta_m{}^{m-1} \cdot f(\pi) = 0)$. The lemma is certainly true for $m = 1$; suppose the lemma true for all $f(x)$ of degree $< m$. Since

$$\phi(x) = f(x) - \delta_m x^m + \delta_m x^{m-1} \pi$$
$$= f(x) - \delta_m x^{m-1}(x - \pi)$$

is of degree $< m$, and $\phi(\pi) = 0$, the polynomial

$$\phi(x)/(x-\pi) = f(x)/(x-\pi) - \delta_m x^{m-1}$$

has coefficients in Z_K. So $f(x)/(x - \pi)$ has coefficients in Z_K.

Corollary: If $f(x)$ is the polynomial of the lemma, and

$$f(x) = \delta_m (x - \pi_1) \ldots (x - \pi_m),$$

then $\delta_m \pi_{i_1} \ldots \pi_{i_k} \in Z_K$ for any $k \leq m$, where $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$.

Proof: By successive applications of the lemma,

$$\frac{f(x)}{(x-\pi_{i_{k+1}})\dots(x-\pi_{i_m})} = \delta_m (X-\pi_{i_1}) \dots (X-\pi_{i_k})$$

has coefficients in Z_K. $\delta_m \pi_{i_1} \dots \pi_{i_k}$ is the last coefficient.

qed

The following is a generalization of Gauss' lemma (lemma 3).

Lemma 48: Let

$$p(x) = \alpha_p X^p + \dots + \alpha_1 X + \alpha_0$$
$$q(x) = \beta_r X^r + \dots + \beta_1 X + \beta_0$$

be polynomials with coefficients in Z_K, $\alpha_p \beta_r \neq 0$. Let

$$r(x) = p(x) \cdot q(x) = \gamma_s X^s + \dots + \gamma_1 X + \gamma_0$$

If $\delta \in Z_K$ such that all $\gamma_h/\delta \in Z_K$, then all $\alpha_i \beta_j/\delta \in Z_K$.

Proof: Suppose

$$p(x) = \alpha_p (x-\tau_1) \dots (x-\tau_p)$$
$$q(x) = \beta_r (x-\sigma_1) \dots (x-\sigma_r)$$

then since $\alpha_p \beta_r = \gamma_s$

$$\frac{r(x)}{\delta} = \frac{\alpha_p \beta_r}{\delta} (x-\tau_1) \dots (x-\tau_p)(x-\sigma_1) \dots (x-\sigma_r)$$

has coefficients in Z_K. The preceding corollary gives that every product

$$\frac{\alpha_p \beta_r}{\delta} \tau_{n_1} \dots \tau_{n_p} \sigma_{m_1} \dots \sigma_{m_q}$$

is in Z_K. But α_i/α_p and β_j/β_r are the elementary symmetric

functions in the τ_i and σ_j respectively, so

$$\frac{\alpha_i \beta_j}{\delta} = \frac{\alpha_\rho \beta_r}{\delta} \cdot \frac{\alpha_i}{\alpha_\rho} \cdot \frac{\beta_j}{\beta_r}$$

is a sum of terms of the form $\frac{\alpha_\rho \beta_r}{\delta} \tau_{n_1} \cdots \tau_{n_f} \sigma_{m_1} \cdots \sigma_{m_g}$

Thus $\alpha_i \beta_j / \delta \in Z_K$

qed

Lemma 49: For every ideal A of Z_K, there is an ideal B and a rational integer a such that $AB = (a)$.

Proof: Let $A = (\alpha_1, \ldots, \alpha_r)$ and define

$$g_i(x) = \alpha_1^{(i)} x + \ldots + \alpha_r^{(i)} x^r ,$$

where $\alpha_j^{(i)}$, $i = 1, \ldots, n$, are the n conjugates of α_j for K ($K = \mathbb{Q}(\theta)$ is of degree n over $\mathbb{Q}$; θ is algebraic over $\mathbb{Q}$). Let

$$F(x) = g_1(x) \cdots g_n(x) = \sum c_p x^p .$$

Show that the coefficients of F(x) are in $\mathbb{Z}$.

If all the conjugates of each α_j are not in K, Adjoin them to K, obtaining a K-extension $L = K(\alpha_1^{(1)}, \alpha_1^{(2)}, \ldots, \alpha_j^{(i)}, \ldots, \alpha_n^{(n-1)}, \alpha_n^{(n)})$. L is finite over K and hence over $\mathbb{Q}$. Each of these α_j then satisfies its minimal polynomial (with coefficients in $\mathbb{Z}$), so they are all in Z_L. The coefficients of F(x) are sums of products of the $\alpha_j^{(i)}$, so, since Z_L is a ring, the coefficients are in Z_L.

Define a mapping σ_2: $L[x] \longrightarrow \mathbb{Q}[x]$: if $f(x) = \beta_m x^m + \ldots + \beta_1 x + \beta_0 \in L[x]$, then

$$\sigma_2(f(x)) = \beta_m^{(2)} x^m + \ldots + \beta_1^{(2)} x + \beta_0^{(2)}$$

By the remarks preceding lemma 22, σ_2 is a homomorphism. If

$$\sigma_2(f(x)) = 0,$$

then $\beta_i^{(2)} = 0$, for all i. But then $\beta_i^{(2)}$ is in $\mathcal{K}$, so that all of its conjugates are the same, namely 0. In particular, $\beta_i = 0$, and so $f(x) = 0$. Thus the kernel of σ_2 is (0), and σ_2 is an isomorphism. By lemma 23(ii), $\sigma_2(f(x)) = f(x)$ if and only if $f(x) \in \mathcal{K}[x]$.

Notice that

$$\sigma_2(g_i(x)) = g_{\pi(i)}(x),$$

(where the mapping $\pi\{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ is a permutation) since conjugacy is an equivalence relation. All $g_{\pi(i)}(x)$ are distinct, for otherwise

$$g_{\pi(i)}(x) = g_{\pi(k)}(x)$$
$$\sigma_2(g_i(x)) = \sigma_2(g_k(x))$$

for some $i \neq k$, which is impossible, since σ_2 is one to one. Thus

$$\begin{aligned}\sigma_2(F(x)) &= \sigma_2(g_1(x) \ldots g_n(x)) \\ &= \sigma_2(g_1(x)) \ldots \sigma_2(g_n(x)) \\ &= g_{\pi(1)}(x) \ldots g_{\pi(n)}(x) \\ &= F(x).\end{aligned}$$

Thus $F(x) \in \mathcal{K}[x]$, and the coefficients of $F(x)$ are in $\mathcal{K}$. But they are also in Z_L, so by lemma 12, they are in $\mathcal{Z}$.

If $g_1(x)$ is the polynomial having the original α_i as coefficients, then $g_1(x) \mid F(x)$, and

$$h(x) = \frac{F(x)}{g_1(x)} = g_2(x) \ldots g_n(x)$$

has coefficients in Z_K. (Since the coefficients of g_1 are in Z_K). Let $h(x) = \beta_1 x + \ldots + \beta_m x^m$. Let a be the GCD (in $\mathbb{Z}$) of c_p, the coefficients of F(x), so that F(x)/a is primitive. Define $B = (\beta_1, \ldots, \beta_m)$ and show that AB = (a).

Since $F(x) = h(x) \cdot g_1(x)$, $a \mid \alpha_i \beta_j$ for all i and j, by the preceding lemma. Thus $(a) \supseteq AB$. On the other hand, since a is the GCD of the c_p, the rational integers c_p/a are relatively prime. Thus there exist rational integers x_p such that

$$1 = \sum x_p \frac{c_p}{a} , \qquad a = \sum x_p c_p .$$

But each c_p is, by the definition of the β_i's, of the form

$$\sum_{i,j} \lambda_{ijp} \alpha_i \beta_j$$

so a is of the form

$$\sum_{i,j} \left(\sum_p x_p \lambda_{ijp} \right) \alpha_i \beta_j .$$

So $a \in AB$, and $(a) = AB$.

qed

Lemma 50: Z_K is a UFD if and only if Z_K is a PID.

Proof: It is well known that any PID is a UFD. It must be shown that if Z_K is a UFD, then every ideal is principal. It suffices to show that every prime ideal $P \neq Z_K$ is principal, due to the theorem.

The preceding lemma guarantees that $P \mid (a)$ for some rational integer a. Let $a = \pi_1 \ldots \pi_r$ be the UF of a in Z_K. Then $(a) = (\pi_1) \ldots (\pi_r)$ so $P \mid (\pi)$, for some prime element of Z_K. By corollary 2 of lemma 42, $(\pi) = PA$, for some ideal

A of Z_K. Notice that $(\pi) \subseteq A$. The corollary to lemma 46 says P and A can be written

$$P = (\pi, \gamma), \qquad A = (\pi, \delta),$$

and

$$(\pi) = PA = (\pi, \gamma)\cdot(\pi, \delta)$$
$$= (\pi^2, \pi\gamma, \pi\delta, \gamma\delta)$$

Thus $\gamma\delta \in (\pi)$, or $\pi \mid \gamma\delta$. UF in Z_K provides $\pi \mid \gamma$ or $\pi \mid \delta$. Show $\pi \nmid \delta$.

If $\pi \mid \delta$, then $A = (\pi, \delta) = (\pi)$, so $(\pi) = PA = P(\pi)$ and $P = (1) = Z_K$. This is impossible by definition of prime ideal. Thus $\pi \nmid \delta$, $\pi \mid \gamma$, and $P = (\pi, \gamma) = (\pi)$, and P is principal. Thus every ideal of Z_K is principal and Z_K is a PID. (Notice that $A = (1)$.)

qed

Finally, a specific example will now be exhibited of an ideal in Z_K represented as a product of prime ideals. Let $K = \mathbb{Q}(\sqrt{10})$, and $Z_K = \mathbb{Z}[\sqrt{10}]$. Every element $\alpha \in K$ is of the form

$$\alpha = (a + b\sqrt{10})/c, \quad a,b,c \in \mathbb{Z}, \quad c \neq 0$$

Since $\mathbb{Q}(\sqrt{10})$ is of degree = 2 over $\mathbb{Q}$, every element of $\mathbb{Q}(\sqrt{10})$ satisfies a monic quadratic polynomial over $\mathbb{Q}$. In particular, if $\alpha \in \mathbb{Q}(\sqrt{10})$, $\alpha = (a + b\sqrt{10})/c$, and $a,b,c \in \mathbb{Z}$, then α satisfies

$$f(x) = x^2 - (2a/c)x + (a^2 - 10b^2)/c^2 = 0.$$

Since $\mathbb{Q}(\sqrt{10}) \subseteq \mathbb{R}$, $f(x) = 0$ can be solved for x, using the quadratic formula:

$$x = \left(2a/c \pm \sqrt{4a^2/c^2 - 4(a^2 - 10b^2)/c^2}\right)/2$$

$$\chi = (1/c)\left(a \pm \sqrt{a^2 - a^2 + 10b^2}\right)$$
$$= (a \pm b\sqrt{10})/c$$

Thus the other conjugate of $(a + b\sqrt{10})/c$ is $(a - b\sqrt{10})/c$, and the norm $N(\alpha)$ of α is:

$$N(\alpha) = \left((a + b\sqrt{10})(a - b\sqrt{10})\right)/c^2$$
$$= (a^2 - 10b^2)/c^2,$$

It is possible that in this case, $Z_K = Z[\sqrt{10}]$ might be a UFD. Doubts are quickly dispelled on observing

$$6 = 2 \cdot 3 = (4 + \sqrt{10}) \cdot (4 - \sqrt{10}).$$

All five of these elements are in $Q(\sqrt{10})$. But it must be shown that 2, 3, $4 + \sqrt{10}$, and $4 - \sqrt{10}$ are prime in order to show that UF does not hold. Notice that $N(2) = 4$, $N(3) = 9$, $N(4 \pm \sqrt{10}) = 6$, so 2, 3, $4 \pm \sqrt{10}$ are not units. If any of these are not prime, then there exist in $Z[\sqrt{10}]$ elements α, β, not units, such that $\alpha\beta = 2$, $\alpha\beta = 3$, or $\alpha\beta = 4 \pm \sqrt{10}$. But then $N(\alpha) \cdot N(\beta) = 4$, $N(\alpha) \cdot N(\beta) = 9$ or $N(\alpha) \cdot N(\beta) = 6$. Since α and β are not units, $N(\alpha) \neq \pm 1$, $N(\beta) \neq \pm 1$. Thus, by UF in Z,

$$N(\alpha) = \pm 2 \text{ or } N(\alpha) = \pm 3$$
$$N(\beta) = \pm 2 \text{ or } N(\beta) = \pm 3.$$

But are there any elements at all of $Z[\sqrt{10}]$ whose norms are ± 2 or ± 3?. That is to say, are there rational integers a and b such that one of the following holds

$$a^2 - 10b^2 = 2, \quad a^2 - 10b^2 = -2$$
$$a^2 - 10b^2 = 3, \quad a^2 - 10b^2 = -3 \quad ?$$

Map the elements in these equations into the ring $Z/10Z$ by the natural homomorphism of $Z \longrightarrow Z/10Z$. Then the equations become

$$\overline{a^2} - \overline{10b^2} = \overline{2}, \quad \overline{a^2} - \overline{10b^2} = \overline{-2} = \overline{8}$$
$$\overline{a^2} - \overline{10b^2} = \overline{3}, \quad \overline{a^2} - \overline{10b^2} = \overline{-3} = \overline{7}$$

or

$$\overline{a^2} = \overline{2}, \quad \overline{a^2} = \overline{8}, \quad \overline{a^2} = \overline{3}, \quad \overline{a^2} = \overline{7}$$

But there are no elements of $Z/10Z$ whose square is 2, 3, 7, or 8. Thus no elements of $Z[\sqrt{10}]$ have norms ± 2 or ± 3, and the elements 2, 3, $4 \pm \sqrt{10}$ are prime. Note too that since the norms of 2 and 3 are different from the norms of $4 \pm \sqrt{10}$, neither 2 nor 3 are associated with either of $4 \pm \sqrt{10}$ (a is associated with b, if and only if $a = bc$, where c is a unit). The element 6 therefore has been factored in two essentially different ways into products of primes, and UF does not hold in $Z[\sqrt{10}]$.

However, it will now be shown that the ideal (6) is a product of prime ideals; namely

$$(6) = P_1^2 P_2 P_3,$$

where $P_1 = (2, \sqrt{10})$, $P_2 = (3, 4 + \sqrt{10})$, $P_3 = (3, 4 - \sqrt{10})$, and P_1, P_2, P_3 are all prime ideals.

First the equality. $P_1^2 = (4, 2\sqrt{10}, 10)$. Thus $P_1^2 = (2)$, since $2|4$, $2|2\sqrt{10}$, and $2|10$; also $10 - 2(4) = 2$. $P_2P_3 = (9, 12 - 3\sqrt{10}, 12 + 3\sqrt{10}, 6)$. $P_2P_3 = (3)$ since 3 divides the four generators of P_2P_3; also $9 - 6 = 3$, where 9 and 6 are in P_2P_3. Thus $(6) = (2)(3) = P_1P_1P_2P_3$.

Are P_1, P_2 and P_3 prime? For P_1, it is evident that $\beta \in P_1$, if $\beta = 2a + \sqrt{10}b$, and $a, b \in Z$. Conversely, let δ be any element of P_1 Then

$$\delta = 2\gamma_1 + \sqrt{10}\,\gamma_2$$

where $\gamma_1, \gamma_2 \in Z[\sqrt{10}]$. Let $\gamma_1 = c_1 + \sqrt{10}d_1$, $\gamma_2 = c_2 + \sqrt{10}d_2$. Then

$$\begin{aligned}\delta &= 2(c_1 + \sqrt{10}d_1) + \sqrt{10}\,(c_2 + \sqrt{10}d_2) \\ &= 2(c_1 + 5d_2) + \sqrt{10}\,(2d_1 + c_2).\end{aligned}$$

$2(c_1 + 5d_1)$ is an even rational integer; so P_1 consists precisely of elements of the form $2a + \sqrt{10}b$, where $a, b \in Z$. i.e. elements whose rational term is even.

To show that P_1 is prime, then, it must be shown that if $\beta_1, \beta_2 \notin P_1$, then $\beta_1\beta_2 \notin P_1$. But $\beta_1, \beta_2 \notin P_1$ implies that the rational terms of β_1 and β_2 are odd; so the rational term of $\beta_1\beta_2$ is odd, and $\beta_1\beta_2 \notin P_1$. Thus P_1 is prime.

For P_3, let $\beta = a + \sqrt{10}b \in Z[\sqrt{10}]$. Show $\beta \in P_3$ if and only if $3 \mid (a + b)$.

Suppose that $a + b = 3k$, $a = 3k - b$. Then

$$\beta = a + \sqrt{10}b = 3(k + b) - (4 - \sqrt{10})b.$$

But 3 and $4 - \sqrt{10}$ are the generators of P_3, so $\beta \in P_3$

Conversely, suppose $\beta \in P_3$. Then

$$\begin{aligned}\beta &= 3(a_1 + \sqrt{10}b_1) + (4 - \sqrt{10})(a_2 + \sqrt{10}b_2) \\ &= (3a_1 + 4a_2 - 10b_2) + \sqrt{10}(3b_1 - a_2 + 4b_2).\end{aligned}$$

If $\beta = a + \sqrt{10}b$, then notice that $3 \mid (a + b)$.

Now if $\beta_1 = a_1 + \sqrt{10}b_1$, and $\beta_2 = a_2 + \sqrt{10}b_2$, and $\beta_1\beta_2 = a + \sqrt{10}b$, then $a = a_1a_2 + 10b_1b_2$, $b = a_1b_2 + b_1a_2$,

and $a + b = (a_1 + b_1)(a_2 + b_2) + 9b_1b_2$. Thus $3 \mid (a + b)$ if and only if $3 \mid (a_1 + b_1)(a_2 + b_2)$. If neither β_1 nor β_2 are in P_3, then 3 divides neither $(a_1 + b_1)$ nor $(a_2 + b_2)$. Thus $3 \nmid (a_1 + b_1)(a_2 + b_2)$ and $3 \nmid (a + b)$. Hence $\beta_1\beta_2 \notin P_3$, and P_3 is prime.

The proof that P_2 is prime goes through in a similar fashion, noting that $\beta = a + b\sqrt{10} \in P_2$ if and only if $3 \mid (a - b)$. Thus $(6) = P_1P_1P_2P_3$ where P_i are prime ideals.

Footnotes

Sources referred to are listed in the Bibliography.

1. Hardy and Wright, pp. 204-208
2. Hardy and Wright, pp. 208-212

4. Adamson, p. 51
5. van der Waarden, v.1, p. 78 ff.
6. Adamson, p. 44
7. Mirsky, p. 17
8. van der Waarden, v.2, p. 73

Sources

Adamson, I. T. : Introduction to Field Theory, London, 1964

Hardy, G. H. and Wright, E. M. : An Introduction to the Theory of Numbers, London, 1938

Herstein, I. N.: Topics in Algebra, New York, 1964

McCoy, N. H.: Rings and Ideals, Menasha, Wisconsin, 1962

Mirsky, L.: An Introduction to Linear Algebra, New York, 1955

Pollard, H.: The Theory of Algebraic Numbers, Baltimore, 1950

Robinson, A.: Numbers and Ideals, San Fransisco, 1965

van der Waarden, B. L.: Modern Algebra, v. 1,2, New York, 1950

Zariski, O and Samuel, P.: Commutative Algebra, v.1, New York, 1965

Throughout this paper, I have received invaluable assistance and instruction from my honors advisor, Mr. R. W. Johnson.