Theorem 1. Let A be an integral domain, and let L be a field containing A. The elements of L integral over A form a ring.

Remark. The immediate consequence of this theorem is that the ring of integers is indeed a ring.

Definition 2. Symmetric polynomials and elementary symmetric polynomials.

Theorem 3. Let A be a ring. Every symmetric polynomial $P(X_1, \ldots, X_r)$ in $A[X_1, \ldots, X_n]$ can be represented with a linear combination of elementary symmetric polynomials with coeffcients in A.

Proof is constructive and inductive by reducing the polynomial over the lexicographically highest monomial. Not a hard proof, but the indecies are anoying.

The above proof implies:

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

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

(I'm not quite sure why this is the case. Maybe use the multi-binomial theorem.)

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

Proposition 4. Let A be a integral domain and Ω be 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 every polynomial $g(\alpha_1, \ldots, \alpha_n)$ in $A[\alpha_1, \ldots, \alpha_n]$ is a root of a monic polynomial in $A[X]$.

Proof. Clearly,

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

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

With this we can prove that the above theorem. I don't quite understand few steps ...

Dedekind's Proof

Proposition 5. Let L be a field containing A. An element α of L is integral over A if and only if there exists a nonzero finitely generated A-submodule of L such that $\alpha M \subset M$ (in fact, we can take $M = A[\alpha]$, the A-subalgebra generated by α).

Proof.

- Let $\alpha \in L$ be integral over A. The A-submodule $A[\alpha]$ in L is generated by $1, \alpha, \ldots, \alpha^{n-1}$, thus finitely generated and clearly nonzero. $\alpha A[\alpha] \subset A[\alpha]$ also holds.
- Let M be a nonzero, finitely generated A-submodule in L such that $\alpha M \subset M$. Since M is finitely generated, there is a set of generators $v_1, \ldots, v_n \in M$. From $\alpha M \subset M$ we have that

$$\alpha v_i = \sum_{j=1}^{n} a_{i,j} v_j$$

for some $a_{i,j} \in A$. We rewrite this system of equations

$$(\alpha - a_{i,i})v_i \sum_{j=1, j\neq i}^{n} a_{i,j} v_j = 0$$

We have the matrix

$$\begin{pmatrix} (\alpha - a_{1,1}) & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & (\alpha - a_{2,2}) & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & (\alpha - a_{n,n}) \end{pmatrix}$$

Applying Cramer's Rule we get $v_i = \frac{\det(C_i)}{\det C}$, but C_i is always 0, and at least one v_i is nonzero, so we have that $\det(C) = 0$.

But calculating the determinant of C gives us

$$\alpha^n + c_1 \alpha^{n-1} + \cdots + c_n = 0$$

as desired.

□

Now take α and β integral over A and denote $\alpha M \subset M$ and $\beta N \subset N$.

1. MN is an A-submodule of L.

Dedekind's proof is much easier to understand, lol.

Integral Elements

Proposition 6. Let K be the field of fractions of A, and let L be a field containing K. If $\alpha \in L$ is algebraic over K, then there exists a nonzero $d \in A$ such that $d\alpha$ is integral over A.

Corollary 1. Let A be an integral domain with field of fractions K, and let B be the integral closure of A in a field L containing K. If L is algebraic over K, then it is the field of fractions B.

Part I

Exercise

Example 6.1. Let d be a square-free integer. Consider $A = \mathbb{Z}[\sqrt{d}]$. Show that every element of R can be written as a product of irreducible elements.

Proof. Define $N : R \longrightarrow \mathbb{N}$ as $N(a+b\sqrt{d}) = |a^2 - db^2|$ where $a, b \in \mathbb{Z}$. Let $a_1 + b_1\sqrt{d}$ and $a_2 + b_2\sqrt{d}$ be two elements in $\mathbb{Z}[\sqrt{d}]$ with $a_1, b_1, a_2, b_2 \in \mathbb{Z}$, then

$$\begin{aligned} N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) &= N((a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}) \\ &= |(a_1a_2 + b_1b_2d)^2 - d(a_1b_2 + a_2b_1)^2| \\ &= |a_1^2a_2^2 + 2a_1a_2b_1b_2d + b_1^2b_2^2d^2 - a_1^2b_2^2d - 2a_1a_2b_1b_2d - a_2^2b_1^2d| \\ &= |a_1^2a_2^2 - a_1^2b_2^2d - a_2^2b_1^2d + b_1^2b_2^2d^2| \end{aligned}$$

on the other hand

$$\begin{aligned} N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d}) &= |a_1^2 - db_1^2||a_2^2 - db_2^2| \\ &= |a_1^2a_2^2 - a_1^2b_2^2d - a_2^2b_1^2d + b_1^2b^2d^2| \end{aligned}$$

so we have $N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) = N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d})$. Moreover, let $u \in \mathbb{Z}[\sqrt{d}]$ be a unit, then there is an element $v \in \mathbb{Z}[\sqrt{d}]$ such that $uv = 1$. Applying the function defined above, we get

$$1 = N(1) = N(uv) = N(u)N(v)$$

so $N(u) = 1$. Now suppose $N(a + b\sqrt{d}) = 1$ with $a, b \in \mathbb{Z}$. Consider

$$(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 = \pm 1$$

and therefore $a + b\sqrt{d}$ is a unit.

We have shown that N is a norm map. R is also an integral domain because if $x \in R$ is a zero-divisor, then we have $0 = N(x) = |a^2 - db^2|$, but this is impossible since d is square-free. Applying the example before, we get the desired result. $\square$