

**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  $P(X_1, \dots, X_r)$  in  $A[X_1, \dots, X_n]$  can be represented with a linear combination of elementary symmetric polynomials with coefficients in  $A$ .

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

The above proof implies:

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

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

(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 an integral domain and  $\Omega$  be an algebraically closed field containing  $A$ . If  $\alpha_1, \dots, \alpha_n$  are the roots in  $\Omega$  of a monic polynomial in  $A[X]$ , then every polynomial  $g(\alpha_1, \dots, \alpha_n)$  in  $A[\alpha_1, \dots, \alpha_n]$  is a root of a monic polynomial in  $A[X]$ .

*Proof.* Clearly,

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

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

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  $\alpha$  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  $\alpha$ ).

*Proof.* • Let  $\alpha \in L$  be integral over  $A$ . The  $A$ -submodule  $A[\alpha]$  in  $L$  is generated by  $1, \alpha, \dots, \alpha^{n-1}$ , 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  $v_1, \dots, v_n \in M$ . 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  $\alpha$  and  $\beta$  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  $N : R \rightarrow \mathbb{N}$  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

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

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.  $\square$

**Example 6.2.** 2.1.3. did it before

**Example 6.3.** Let  $R$  be a domain in which every element can be written as a product of irreducibles. Show that the following are equivalent.

1. this factorization is unique
2. if  $\pi$  is irreducible and  $\pi$  divides  $ab$ , then  $\pi|a$  or  $\pi|b$

*Proof.* Let the factorization be unique,  $\pi \in R$  be irreducible and divide  $ab$ . Then  $ab = \pi x$  for some  $x \in R$ . On the other hand,  $ab$  has a unique factorization that is the product of the factorization of  $a$  and  $b$  but must contain  $\pi$ .

For the other side let  $p_1^{r_1} \cdots p_n^{r_n}$  and  $q_1^{s_1} \cdots q_m^{s_m}$  be two factorizations of an element in  $R$ . Then  $p_1$  divides  $q_1^{s_1} \cdots q_m^{s_m}$  so  $p_1$  divides some  $q_i$ . But  $q_i$  is irreducible, so we have  $p_1 = q_i$ . Induction yields the desired result.  $\square$

**Example 6.4.** Show that if  $\pi$  is an irreducible element of a principal ideal domain, then  $(\pi)$  is a maximal ideal.

*Proof.* Assume  $(\pi)$  is not maximal, then there is an ideal  $(a)$  with  $a \neq 1$  such that  $(\pi) \subsetneq (a)$ . But this implies  $\pi = ra$  for some  $r \in R$  that is not a unit. This is a contradiction.  $\square$

**Example 6.5.** If  $F$  is a field, prove that  $F[x]$  is Euclidean.

*Proof.* Define  $\phi : F[x] \rightarrow \mathbb{N}$  as  $\phi(f) = \deg(f)$ . Fix two polynomials  $f, g \in F[x]$ . If  $\deg(f) \geq \deg(g)$ , then we can do polynomial division to get  $f = gp + r$  where  $\deg(r) < \deg(g)$ .  $\square$

**Example 6.6.** Show that  $\mathbb{Z}[i]$  is Euclidean.

*Proof.* Fix two elements  $x, y \in \mathbb{Z}[i]$  and write  $x = a_x + ib_x$  and  $y = a_y + ib_y$ . It is

$$\frac{x}{y} = \underbrace{\frac{a_x a_y + b_x b_y}{a_y^2 + b_y^2}}_{=: \alpha} + i \underbrace{\frac{a_y b_x - a_x b_y}{a_y^2 + b_y^2}}_{=: \beta}$$

Set  $p_x$  to be the closest integer to  $\alpha$  and  $p_y$  to be the closest integer to  $\beta$  and  $p = p_x + ip_y$ . Moreover, set  $r = ((\alpha - p_x) + i(\beta - p_y))y$ .

It is

$$\begin{aligned} r &= y(\alpha + i\beta) - y(p_x + ip_y) \\ &= y \frac{x}{y} - py \\ &= x - py \end{aligned}$$

so we got the desired representation.

Furthermore, we have

$$\begin{aligned} N(r) &= N(y)((\alpha - p_x)^2 + (\beta - p_y)^2) \\ &\leq N(y) \frac{1}{2} \end{aligned}$$

□