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 $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$, 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. $\square$

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 π is irreducible and π 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 π.

For the other side let $p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}$ and $q_1^{s_1} \cdot \ldots \cdot q_m^{r_m}$ be two factorizations of an element in R. Then p_1 divides $q_1^{s_1} \cdot \ldots \cdot q_m^{r_m}$ 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 π is an irreducible element of a principal ideal domain, then (π) is a maximal ideal.

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

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 α and p_y to be the closest integer to β 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

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

□

Example 6.7. Prove that if p is a positive prime, then there is an element $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv -1 \mod p$ if and only if either $p = 2$ or $p \equiv 1 \mod 4$.

Proof.

1. Let $p = 2$, then we can simply choose $x = 1$. Now let $p \equiv 1 \mod 4$. With Wilson's Theorem we have

$$-1 \equiv (p-1)! \equiv 1 \cdot \ldots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot p \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \cdot (-1)^{\frac{p-1}{2}} \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2$$

where $\mod p$. So choose the last expression as x and we are done.

2. If $p = 2$, then we are done. Now let $x^2 \equiv -1 \mod p$. If $p \equiv 3 \mod (4)$, we have

$$x^{p-1} = x^{4n+2} = x^{4n}x^2 \equiv -1(x^4)^n \equiv -1 \mod p$$

as $x^4 \equiv 1 \mod p$. But this contradicts Fermat's Little Theorem.

□

Example 6.8. Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$.

Proof. If x is even, then $4|x^3$, so $x^3 - 1 \equiv 3 \mod 4$ which cannot be a square since all squares are congruent to either 0 or 1 $\mod 4$. So x is odd and y is even. Write $y^2 + 1 = (y+i)(y-i)$. If a prime divides $(y+i)(y-i)$, then the prime divides also their difference $2i$. So $p = 2$ up to units. But then p divides y as y was even, but this is impossible since p also divides $y + i$. □

Example 6.9. What are the primes of $\mathbb{Z}[i]$?

Proof. We have two types of primes in $\mathbb{Z}[i]$.

1. p and ip where $p \equiv 3 \mod 4$.
2. $a + ib$ with $a^2 + b^2 \equiv 1 \mod 4$ and prime.

This is because of the norm function $N(a + ib) = a^2 + b^2$. □

Example 6.10. A positive integer a is the sum of two squares if and only if $a = b^2c$ where c is not divisible by any positive prime $p \equiv 3 \mod 4$.

Proof. I don't know. ∎

Example 6.11. $\mathbb{Z}[\rho]$ is a ring where

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

Proof.

1. $(\mathbb{Z}[\rho], +)$ is an abelian group.
   (a) If $a_1+b_1\rho$ and $a_2+b_2\rho$ are elements of $\mathbb{Z}[\rho]$, then $a_1+b_1\rho+a_2+b_2\rho = a_1+a_2+(b_1+b_2)\rho$, so the addition is well-defined.
   (b) Associativity and commutativity is inhereted from the addition of integers.
   (c) The additive identity is 0.
   (d) If $a+b\rho$ is in $\mathbb{Z}[\rho]$, then its inverse is $-a-b\rho$.
2. $(\mathbb{Z}[\rho], \cdot)$ is a monoid.
   (a) If $a_1+b_1\rho$ and $a_2+b_2\rho$ are two elements of $\mathbb{Z}[\rho]$, then we have

$$\begin{aligned}(a_1+b_1\rho)(a_2+b_2\rho) &= a_1a_2 + b_1b_2\rho^2 + (a_1b_2+a_2b_1)\rho \\ &= a_1a_2 + b_1b_2\overline{\rho} + (a_1b_2+a_2b_1)\rho \\ &= a_1a_2 + b_1b_2\frac{-1-\sqrt{3}}{2} + (a_1b_2+a_2b_1)\frac{-1+\sqrt{3}}{2} \\ &= a_1a_2 - \frac{b_1b_2}{2} - \frac{a_1b_2+a_2b_1}{2} - \frac{b_1b_2\sqrt{-3}}{2} + \frac{(a_1b_2+a_2b_1)\sqrt{-3}}{2} \\ &= a_1a_2 + \frac{-a_1b_2-a_2b_2-b_1b_2}{2} + \frac{(a_1b_2+a_2b_1-b_1b_2)\sqrt{-3}}{2}\end{aligned}$$

   I made some mistake, but should be right.
   (b) The multiplicative identity is 1
3. Distributive law is again inherited.

∎

Example 6.12.

1. Show that $\mathbb{Z}[\rho]$ is Euclidean.

   Proof. Fix two elements $x_1+x_2\rho$ and $y_1+y_2\rho$ of $\mathbb{Z}[\rho]$. We have

$$\begin{aligned}\frac{x_1+x_2\rho}{y_1+y_2\rho} &= \frac{x_1+x_2\rho}{y_1+y_2\rho}\frac{y_1-y_2\rho}{y_1-y_2\rho} \\ &= \frac{x_1y_1 - x_2y_2\overline{\rho} - x_1y_2\rho + x_2y_1\rho}{y_1^2+y_2^2\overline{\rho}}\end{aligned}$$

   I think this should work at the end of the day, but I'm too lazy to write it out. ∎
2. Show that the only units in $\mathbb{Z}[\rho]$ are ± 1, $\pm\rho$, and $\pm\overline{\rho}$.

Chapter 1

Algebraic Numbers and Integers

Example 6.13. Show that
$$\alpha := \frac{\sqrt{2}}{3}$$
is an algebraic number, but not an algebraic integer.

Proof. First of all, α is the root of
$$X^2 - \frac{2}{9} \in \mathbb{Q}[X],$$
so it is an algebraic number.

Now assume α is an algebraic integer. Then, there is a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. It is

$$f(\alpha) = \left(\frac{\sqrt{2}}{3}\right)^n + a_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \cdots + a_1\frac{\sqrt{2}}{3} + a_0 = 0$$
$$(\sqrt{2})^n + 3a_{n-1}(\sqrt{2})^{n-1} + \cdots + 3^{n-1}a_1\sqrt{2} + 3^n a_0 = 0$$

If n is odd, then $\sqrt{2}$ is not an integer, therefore, we can separate the sum into two smaller ones.

$$\sum_{k \text{ even}} 3^{n-k}a_k(\sqrt{2})^k = 0$$

and

$$\sum_{k \text{ odd}} 3^{n-k}a_k(\sqrt{2})^k = \sqrt{2}\sum_{k \text{ even}} 3^{n-k}a_k(\sqrt{2})^{\frac{k-1}{2}} = 0.$$

Both sums are divisible by 3 as 3 divides 0 and since all summands except for the very last one contains multiples of 3, they are divisible by 3, so the last summand must be divisible by 3 as well. But this cannot be. Hence α is not an algebraic integer. $\square$

Example 6.14. Show that if $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

Proof. Write $r = \frac{p}{q}$ such that $q \not| p$ and we have

$$p^n + qa_{n-1}p^{n-1} + \cdots + q^n a_0 = 0$$

q divides the whole sum, it divides all summands, but it does not divide p^n, therefore $q = 1$. $\square$

Chapter 2

Integral Bases

Lemma 7. If K is an algebraic number field of degree n over $\mathbb{Q}$, and $\alpha \in \mathcal{O}_K$ its ring of integers, then $\mathrm{Tr}_K(\alpha)$ and $\mathrm{N}_K(\alpha)$ are in $\mathbb{Z}$.

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Q}$-basis for K, then for all $1 \leq i \leq n$ it is

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j.$$

Then we have for all $1 \leq i \leq n$ and k

$$\alpha^{(k)}\omega_i^{(k)} = \sum_{j=1}^{n} a_{i,j}\omega_j^{(k)}$$

where $\alpha^{(k)}$ is the k-th conjugate of α.

Missing, but I kinda get it. $\square$

Example 7.1.