I. Algebraic Integers

1. Motivation

At its most elementary, number theory is the study of integers. Few topics:

- primes;
- integer equations;
- divisibility;
- gcd; and
- prime factorization.

The goal is to generalize these topics with *commutative algebra*.

Naive approach is to use UFD's. A problem with this is that there are many *integer-like* integral domains, such as $\mathbb{Z}\left[\sqrt{5}\right]$, that are not UFD's.

Let us do some *random* math and see where it goes. Consider

$$\alpha = \frac{1+\sqrt{5}}{2}.$$

Note that $\alpha \in \mathbb{Q}\left[\sqrt{5}\right]$. In fact, observe that α is the root of the polynomial $x^2 - x - 1$, so that

$$\alpha^2 = \alpha + 1. \tag{1.1}$$

Def'n 1.1. $\mathbb{Z}[\alpha]$

Given $\alpha \in \mathbb{C}$, define

$$\mathbb{Z}[\alpha] = \{f(\alpha) : f \in \mathbb{Z}[x]\}.$$

For the specific $\alpha = \frac{1+\sqrt{5}}{2}$, observe that [1.1] tells us that we can replace any α^2 with a linear polynomial in α, so that

$$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\}.$$

This simplification worked because

$$\textit{there is a monic } f \in \mathbb{Z}[x] \textit{ such that } f(\alpha) = 0.$$

In fact, observe that $\alpha = \frac{1+\sqrt{5}}{2}$ implies that

$$(2\alpha - 1)^2 = 5,$$

which means if we have any other number *congruent to* 5 *mod* 4 in place of 5, we would still get a polynomial of the form

$$4\alpha^2 - 4\alpha - b = 0,$$

where $b \equiv 0 \mod 4$.

The last thing we note about $\mathbb{Z}[\alpha]$ is that

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\,\alpha.$$

In general, we want to have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\,\alpha + \cdots + \mathbb{Z}\,\alpha^{n-1}$$

which allows us to do $\mathbb{Z}$-*module theory*.

2. Algebraic Integers

Def'n 1.2. **Algebraic Integer**
We say $\alpha \in \mathbb{C}$ is an ***algebraic integer*** if and only if there exists a monic $f \in \mathbb{Z}[x]$ such that

$$f(\alpha) = 0.$$

We do not insist that f is irreducible. For instance, $7, \sqrt{5}, \frac{1+\sqrt{5}}{2}, i, 1+i, \zeta_n$ are all algebraic integers, where ζ_n is an nth root of unity.

How do we tell if an *algebraic number* $\alpha \in \mathbb{C}$ (i.e. α is a root of a not-necessarily monic polynomial over $\mathbb{Z}$) is an algebraic integer?

Theorem 1.1.
An algebraic number $\alpha \in \mathbb{C}$ is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ is over $\mathbb{Z}$.

Postponed

Corollary 1.1.1.
The only algebraic integers in $\mathbb{Q}$ are integers.

Example 1.1.
Consider

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

Then $(2\beta - 1)^2 = 3$, so that β is a root for

$$f = x^2 - x - \frac{1}{2}.$$

But f is a monic polynomial with $\deg(f) = 2$ and a root β of f is irrational, it follows that f is the minimal polynomial for β over $\mathbb{Q}$. Thus β is not an algebraic integer.

Suppose that

$$f = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x].$$

Then the ***content*** of f is

$$\text{content}(f) = \gcd(a_0, \ldots, a_n)$$

and we say that

$$f \text{ is } \textbf{\textit{primitive}} \iff \text{content}(f) = 1.$$

In this setting, Gauss's lemma can be stated as following.

Lemma 1.2. Gauss's Lemma
Let $f, g \in \mathbb{Z}[x]$. If f, g are primitive, then so is fg.

Proof of Theorem 1.1
($\Longleftarrow$) This direction is trivial, as any minimal polynomial is monic.

($\Longrightarrow$) Let $\alpha \in \mathbb{C}$ be an algebraic integer and let $m \in \mathbb{Q}[x]$ be its minimal polynomial. Let $f \in \mathbb{Z}[x]$ be monic such that $f(\alpha) = 0$. Since m is the minimal polynomial,

$$f = mg$$

for some $g \in \mathbb{Q}[x]$.

Take $N_1, N_2 \in \mathbb{N}$ be the smallest positive integers such that $N_1 m, N_2 g \in \mathbb{Z}[x]$. If $p \in \mathbb{N}$ is a prime dividing all coefficients of $N_1 m$, then $\frac{N_1}{p} m \in \mathbb{Z}[x]$. In fact, $\frac{N_1}{p} \in \mathbb{Z}$, since m is monic so that the leading coefficient of $N_1 m$ is N_1. This leads to a contradiction, as $\frac{N_1}{p} < N_1$ violates minimality of N_1.

Also note that f, m are monic, so that g is monic as well. Hence by following a similar argument, $N_2 g$ is primitive.

Now,

$$N_1 N_2 f = (N_1 m)(N_2 g)$$

Since f is monic, observe that the content of $N_1 N_2 f$ is $N_1 N_2$. But $N_1 m, N_2 g$ are primitive, so by Gauss's lemma, $(N_1 m)(N_2 g)$ is primitive. Therefore

$$N_1 N_2 = \text{content}(N_1 N_2 f) = \text{content}((N_1 m)(N_2 g)) = 1,$$

which means $N_1 = N_2 = 1$. Thus $m \in \mathbb{Z}[x]$.

QED

3. Ring of Integers

Example 1.2.

Let $d \in \mathbb{Z}$ be ***square-free*** and $d \neq 1$. That is, in the prime factorization of d, there are no multiplicities. Consider

$$K = \mathbb{Q}\left(\sqrt{d}\right) = \left\{a + b\sqrt{d} : a, b \in \mathbb{Q}\right\}.$$

Then we know that

$$K/\mathbb{Q} \text{ is finite} \implies K/\mathbb{Q} \text{ is algebraic.}$$

We are going to find all algebraic integers in K. Let

$$\alpha = a + b\sqrt{d} \in K$$

be an algebraic integer. Consider the conjugate

$$\overline{\alpha} = a - b\sqrt{d}.$$

Then

$$m = (x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + a^2 - db^2$$

is the minimal polynomial for α over $\mathbb{Q}$. By Theorem 1.1, it follows that $2a, a^2 - db^2 \in \mathbb{Z}$. Now,

$$4\left(a^2 - db^2\right) = (2a)^2 - d(2b)^2$$

but $a^2 - db^2, (2a)^2 \in \mathbb{Z}$, so that

$$d(2b)^2 \in \mathbb{Z}.$$

Since d is square-free, it follows that $2b \in \mathbb{Z}$. If not, then the denominator of $2b$ is not 1. This means the denominator of $(2b)^2$ has a square of a prime as a factor, which contradicts the fact that d is square-free. Hence $\gamma = 2a, \delta = 2b \in \mathbb{Z}$. This means

$$a^2 - db^2 = \left(\frac{\gamma}{2}\right)^2 - d\left(\frac{\delta}{2}\right)^2 = \frac{\gamma^2 - d\delta^2}{4} \in \mathbb{Z}.$$

It follows $\gamma^2 - d\delta^2 \equiv 0 \mod 4$.

We have few cases.

Case 1. $d \equiv 1 \mod 4$.

It follows that

$$\gamma^2 \equiv \delta^2 \mod 4.$$

But even numbers square to 0 mod 4 and odd numbers square to 1 mod 4. Hence

$$\gamma \equiv \delta \mod 2.$$

It follows that α is of the form

$$\alpha = a + b\sqrt{d} = \frac{\gamma + \delta\sqrt{d}}{2}$$

for some $\gamma, \delta \in \mathbb{Z}$.

(End of Case 1)

Case 2. $d \equiv 2 \mod 4$ or $d \equiv 3 \mod 4$.

It is a routine exercise to show that

$$\gamma^2 - d\delta^2 \equiv 0 \mod 4 \iff \gamma \equiv \delta \equiv 0 \mod 2.$$

Hence

$$\alpha = \frac{\gamma}{2} + \frac{\delta}{2}\sqrt{d}$$

but γ, δ are even numbers, so that $a = \frac{\gamma}{2}, b = \frac{\delta}{2} \in \mathbb{Z}$ and

$$\alpha = a + b\sqrt{d}.$$

(End of Case 2)

Exercise: check these conditions are also sufficient.

The above example gives the following idea.

Given a finite extension $K/\mathbb{Q}$, we find all algebraic integers in K.

This motivates the following definitions.

Def'n 1.3. **Number Field**, **Ring of Integers** of a Number Field

We call a finite extension K of $\mathbb{Q}$ a ***number field***.

Given a number field K, we call

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ is an algebraic integer}\}$$

the ***ring of integers*** of K.

We are going to prive that $\mathcal{O}_K$ is a ring.[1] To do so, we first show

$$\mathbb{A} = \{z \in \mathbb{C} : z \text{ is an algebraic integer}\}$$

is a ring, so that

$$\mathcal{O}_K = \mathbb{A} \cap K$$

is also a ring.

Recall that, given $\alpha \in \mathbb{A}$, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}.$$

This allows us to do module theory over $\mathbb{Z}$.

Def'n 1.4. R-**module**

Let R be a ring. An R-***module*** is an abelian group $(M, +)$ with a left R-action on M such that

(a) $1m = m$ for $m \in M$;

(b) $(r_1 + r_2)m = r_1 m + r_2 m$ for $r_1, r_2 \in R, m \in M$;

(c) $r(m_1 + m_2) = rm_1 + rm_2$ for $r \in R, m_1, m_2 \in M$; and

(d) $(r_1 r_2)m = r_1(r_2 m)$ for $r_1, r_2 \in R, m \in M$.

[1] We are going to assume that every ring is unital and commutative throughout, if not stated otherwise.

Example 1.3. Examples of R-modules

Given a ring R, R is an R-module with left action

$$r \cdot m = rm, \qquad \forall r, m \in R.$$

In fact, given any subring $S \subseteq \mathbb{R}$, R is an S-module with

$$s \cdot r = sr, \qquad \forall s \in S, r \in R.$$

Similar to $\mathbb{R}^n$ which is a $\mathbb{R}$-vector space, R^n is an R-module with

$$r \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} rx_1 \\ \vdots \\ rx_n \end{bmatrix}, \qquad \forall r \in R, \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in R^n.$$

Example 1.4.

Consider $R = \mathbb{Z}$ and consider an R-module M. Then given $n \in \mathbb{N}, m \in M$,

$$n \cdot m = (1 + \cdots + 1) \cdot m = 1 \cdot m + \cdots + 1 \cdot m = m + \cdot + m = nm.$$

That is, the $\mathbb{Z}$-module on an abelian group M *does not impose any additional structure on* M; a $\mathbb{Z}$-module is simply an abelian group.

As an exercise, we can also check that

$$(-n) \cdot m = -nm$$

for $n \in \mathbb{N}, m \in M$.

Def'n 1.5. R-**submodule**, **Homomorphism** of R-modules, **Finitely Generated** R-module

Let R be a ring and let M be an R-module. We say $N \subseteq M$ is an R-submodule of M if N is an R-module using the same operations as M.

Given R-modules M, N, we say $f : M \to N$ is a ***homomorphism*** if and only if

$$f(rm_1 + m_2) = rf(m_1) + f(m_2), \qquad \forall r \in R, m_1, m_2 \in M.$$

In case f is bijective, we say f is an ***isomorphism***.

We say an R-module is ***finitely generated*** if there are $m_1, \ldots, m_n \in M$ such that

$$M = Rm_1 + \cdots + Rm_n.$$

That is, for any $m \in M$, there exists $r_1, \ldots, r_n \in R$ such that

$$m = \sum_{j=1}^{n} r_j m_j.$$

In other words, finite number of elements $m_1, \ldots, m_n$ ***generate*** M.

Observe that

$$N \subseteq M \text{ is an } R\text{-submodule} \iff N \text{ is subgroup of } M \text{ closed under } R\text{-left action.}$$

Example 1.5.

Given a ring R, as an R-module, the only R-submodules are the ideals of R.

Def'n 1.6. **Integral** over R

Let R, S be integral domains, such that R is a subring of S. We say $\alpha \in S$ is ***integral*** over R if there is monic $f \in R[x]$ such that $f(\alpha) = 0$.

Example 1.6.

In case $R = \mathbb{Z}, S = \mathbb{C}$, given $\alpha \in S$,

$$\alpha \text{ is integral} \iff \alpha \text{ is algebraic integer.}$$

That is, being integral over R is a generalization of being an algebraic integer.

Theorem 1.3.

Let R, S be integral domains where R is a subring of S and let $\alpha \in S$. Then

$$\alpha \text{ is integral over } R \iff R[\alpha] = \{f(\alpha) : f \in R[x]\} \text{ is a finitely generated } R\text{-module.}$$

Proof. ($\Longrightarrow$) Suppose α is integral over R. Then there is a polynomial relation

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

for some $a_0, \ldots, a_{n-1} \in R$. Rearranging for α^n,

$$\alpha^n = -\left(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right).$$

This means, given any $f \in R[x]$, every powers $\alpha^n, \alpha^{n+1}, \ldots$ in $f(\alpha)$ can be replaced by lower powers of α, so that

$$f(\alpha) = g(\alpha)$$

for some $g \in R[x]$ with $\deg(g) \leq n-1$. That is,

$$R[\alpha] \subseteq R + R\alpha + \cdots + R\alpha^{n-1}.$$

But the reverse containment is trivial, so that $R[\alpha]$ is finitely generated.

($\Longleftarrow$) Suppose $R[\alpha]$ is finitely generated, say

$$R[\alpha] = Rf_1(\alpha) + \cdots + Rf_n(\alpha)$$

with $f_1, \ldots, f_n \in R[x]$. Take $N = \max_{1 \leq j \leq n} \deg\left(f_j\right)$. Then $\alpha^{N+1} \in R[x]$ as a polynomial of α, so that

$$\alpha^{N+1} = \sum_{j=1}^{n} r_j f_j(\alpha)$$

for some $r_1, \ldots, r_n \in R$.

Now consider

$$g = x^{N+1} - \sum_{j=1}^{n} r_j f_j \in R[x].$$

Then $g(\alpha) = 0$. But $\deg\left(x^{N+1}\right) = N+1 > N = \max_{1 \leq j \leq n} \deg\left(f_j\right)$, so that g is monic as well. Thus α is algebraic over R.

QED

The big idea for Theorem 1.3 is that

*showing $\mathbb{Z}[\alpha]$ is finitely generated is often **easier** than finding monic $f \in \mathbb{Z}[x]$ with $f(\alpha) = 0$.*

"Let's work with generators instead of polynomials" - Blake.

Theorem 1.4.
Let
$$\mathbb{A} = \{z \in \mathbb{C} : z \text{ is an algebraic integer}\}.$$
Then $\mathbb{A}$ is a subring of $\mathbb{C}$.

Proof Attempt. If we are in PMATH 348, proving something is *easy*; we simply apply the subring test. Let's see how it fails here.

Let $\alpha, \beta \in \mathbb{A}$. We must show that $\alpha - \beta, \alpha\beta \in \mathbb{A}$. That is, we must show
$$\mathbb{Z}[\alpha - \beta], \mathbb{Z}[\alpha\beta] \text{ are finitely generated } \mathbb{Z}\text{-modules.}$$
Since α, β are algebraic integers, write
$$\mathbb{Z}[\alpha] = \sum_{j=1}^{n} \mathbb{Z}\,\alpha_j, \quad \mathbb{Z}[\beta] = \sum_{j=1}^{m} \mathbb{Z}\,\beta_j.$$
Therefore,
$$\mathbb{Z}[\alpha, \beta] = \{f(\alpha, \beta) : \mathbb{Z}[x, y]\}$$
is also finitely generated. In fact, it is generated by $\left\{\alpha_i\beta_j\right\}_{1\leq i\leq n, 1\leq j\leq m}$. Hence $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module.

We have that $\mathbb{Z}[\alpha - \beta], \mathbb{Z}[\alpha\beta]$ are $\mathbb{Z}$-submodules of the *fg* module $\mathbb{Z}[\alpha, \beta]$.

Now, if we use the intuition from linear algebra, we should be done here. Recall that subspaces of a finite-dimensional vector space are finite-dimensional. But this is not the case for modules!

Proof Failed

Example 1.7. Submodule of a Finitely Generated Module That Is Not Finitely Generated
Consider
$$R = [x_1, x_2, \ldots].$$
Then R is a finitely generated R-module (i.e. $R = R1$). But observe that
$$I = \langle x_1, x_2, \ldots\rangle$$
is not finitely generated.

To see this, observe that elements of R are polynomials in $x_1, x_2, \ldots$, which has *only finitely many indeterminates*. So having finitely many polynomials does not give enough number of indeterminates to generate I.

To resolve this issue, we consider the following definition.

Def'n 1.7. **Noetherian** Ring
Let R be a ring. We say R is ***Noetherian*** if every R-submodule (i.e. ideal) of R is finitely generated.

Example 1.8.
Observe that $\mathbb{Z}$ is Noetherian, as it is a PID (i.e. every ideal of $\mathbb{Z}$ is generated by *an* element).

Theorem 1.5.
Let R be a Noetherian ring and let M be a finitely generated R-module. Then every R-submodule of M is finitely generated.

Theorem 1.5 resolves the issue we left in Theorem 1.4, since $\mathbb{Z}$ is Noetherian.

Let us reduce Theorem 1.5 a bit. Consider a finitely generated R-module
$$M = R\alpha_1 + \cdots + R\alpha_n$$

and an epimorphism of R-modules

$$\begin{aligned} f: R^n &\to M \\ (r_1, \dots, r_n) &\mapsto r_1\alpha_1 + \dots + r_n\alpha_n \end{aligned}.$$

That is, every finitely generated R-module can be viewed as an R-submodule of R^n.

Moreover, for any R-submodule $N \subseteq M$,

$$f^{-1}(N) \subseteq R^n.$$

If $f^{-1}(N) = R\beta_1 + \dots + R\beta_m$, then

$$N = Rf(\beta_1) + \dots + Rf(\beta_m).$$

Hence it remains to show that every R-submodule N of M satisfy $f^{-1}(N) = R\beta_1 + \dots + R\beta_m$ for some $\beta_1, \dots, \beta_m \in R$.

Proof of Theorem 1.5

We may assume $M = R^n$. If $n = 1$, then R is Noetherian and we are done.

Suppose that the result holds for some $n \geq 1$ and consider $M = R^{n+1}$. Consider the epimorphism

$$\begin{aligned} \pi : R^{n+1} &\to R \\ (r_1, \dots, r_{n+1}) &\mapsto r_{n+1} \end{aligned}.$$

Let N be an R-submodule of M. Consider

$$N_1 = \{(r_1, \dots, r_{n+1}) \in N : r_{n+1} = 0\}$$

which is isomorphic to an R-submodule of R^n. Hence by inductive hypothesis, N_1 is finitely generated. Moreover,

$$N_2 = \pi(N)$$

is an R-submodule of R, so is finitely generated (by inductive hypothesis).

Say

$$\begin{aligned} N_1 &= Rx_1 + \dots + Rx_p \\ N_2 &= R\pi(y_1) + \dots + R\pi(y_q) \end{aligned}$$

for some $x_1, \dots, x_p, y_1, \dots, y_q \in R$. Let $x \in N$. Then

$$\pi(x) = r_1\pi(y_1) + \dots + r_q\pi(y_q)$$

for some $r_1, \dots, r_q \in R$. But π is a homomorphism of R-modules, so that

$$\pi\left(x - \sum_{j=1}^{q} r_j y_j\right) = 0.$$

This means the $(n+1)$th entry of $x - \sum_{j=1}^{q} r_j y_j$ is 0, so that $x - \sum_{j=1}^{q} r_j y_j \in N_1$. That is,

$$x - \sum_{j=1}^{q} r_j y_j = \sum_{k=1}^{p} s_k x_k$$

for some $s_1, \dots, s_p \in R$.

Thus

$$x = \sum_{j=1}^{q} r_j y_j + \sum_{k=1}^{p} s_k x_k,$$

so that

$$N = \sum_{j=1}^{q} Ry_j + \sum_{k=1}^{p} Rx_k,$$

as required.

QED

4. Additive Structure

So far, it has been very useful to consider $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Let us investigate this $\mathbb{Z}$-module as an abelian group

$$(\mathcal{O}_K, +)$$

without multiplication structure, where K is a number ring (i.e. $[K : \mathbb{Q}] < \infty$).

The next definition will make it clear the kind of *linear algebraic* approach we are going to take.

Def'n 1.8. **Linearly Independent** Subset of an R-module, **Basis** for an R-module, **Free** R-module
Let R be a ring and let M be an R-module. Let $B \subseteq M$.

(a) Say B is ***linearly independent*** if and only if for all $m_1, \ldots, m_n \in B, r_1, \ldots, r_n \in R$,

$$r_1 m_1 + \cdots + r_n m_n = 0 \implies r_1 = \cdots = r_n = 0.$$

(b) Say B ***spans*** M if for all $x \in M$, there are $b_1, \ldots, b_n \in B, r_1, \ldots, r_n \in R$ such that

$$x = r_1 b_1 + \cdots + r_n b_n.$$

(c) Say B is a ***basis*** for M if B is linearly independent and spans M. In case M admits a basis, we call it a ***free*** R-module.

In case there is a basis B for M, the size of any other basis for M is $|B|$.

Def'n 1.9. **Rank** of a Free R-module
Let R be a ring and let M be a free R-module. Then the size of a basis for M is called the ***rank*** of M, denoted as $\operatorname{rank}(M)$.

Proposition 1.6.

Let R be a ring and let M be an R-module. Let $B \subseteq M$. Then

$$B \text{ is a basis} \iff \text{every } x \in M \text{ can be uniquely written as an } R\text{-linear combination of elements of } B.$$

In particular,

$$M \text{ is free with } \operatorname{rank}(M) = n < \infty \iff M \cong R^n \text{ by } (r_1, \ldots, r_n) \leftrightarrow r_1 b_1 + \cdots + r_n b_n \text{ for some } b_1, \ldots, b_n \in M,$$

in which case $\{b_1, \ldots, b_n\}$ is a basis for M.

Example 1.9. Free but not Finitely Generated

Consider $R = \mathbb{Z}, M = \mathbb{Z}[x], B = \{1, x, x_2, \ldots\}$. Then M is a free module generated by B but is not finitely generated.

Example 1.10. Finitely Generated but not Free

Consider $R = \mathbb{Z}, M = \mathbb{Z}_2$. Then $2 \cdot 1 = 0$ but $2 \neq 0$ in R. So the only R-linearly independent subset of M is the emptyset $\emptyset$, so that M is fintely generated but not free.

Example 1.11.

Consider $R = \mathbb{Z}, M = \mathbb{Z} \times \mathbb{Z}, N = \mathbb{Z} \times 2\mathbb{Z}$. Then M is free with a basis

$$B_1 = \{(1, 0), (0, 1)\},$$

so that $\operatorname{rank}(M) = 2$. Also, N is free with a basis

$$B_2 = \{(1, 0), (0, 2)\},$$

so that $\operatorname{rank}(N) = 2$. However, observe that B_2 is an R-linearly independent subset of M with $\operatorname{rank}(M)$ elements!

This particular example shows that it is possible for modules of rank n to have a linearly independent subset of n elements which does not span the whole module, unlike the case in linear algebra.

We are going to present two facts without proof. Fix a PID R and a free R-module M with $\text{rank}\,(M) = n < \infty$.

Fact 1.7.
For an R-submodule $N \subseteq M$, N is free with $\text{rank}\,(N) \leq n$.

Fact 1.8.
Any maximal linearly independent subset of M has n elements.

The next goal is to show that ring of integers is a free module. That is, given a number field K with $[K : \mathbb{Q}] = n$, our goal is

to find an embedding (i.e. monomorphism) $\varphi : \mathcal{O}_K \to \mathbb{Z}^n$ *such that* $\text{rank}\,(\varphi(\mathcal{O}_K)) = n$.

This will tell us $\mathcal{O}_k \cong \mathbb{Z}^n$ as $\mathbb{Z}$-modules. In particular, $(\mathcal{O}_K, +)$ is a free module with rank n.

Def'n 1.10. **Integral Basis**
Given a free $\mathbb{Z}$-module M, a basis for M is called an ***integral basis***.

We introduce two useful tools in algebraic number theory.

Def'n 1.11. **Trace**, **Norm** of an Element of a Number Field
Let K be a number field with $[K : \mathbb{Q}] = n < \infty$. Let $\alpha \in K$ and consider

$$\begin{aligned} T_\alpha : K &\to K \\ x &\mapsto \alpha x \end{aligned},$$

which is a $\mathbb{Q}$-linear operator.

(a) The ***trace*** of α relative to $K/\mathbb{Q}$, denoted as $\text{tr}_{K/\mathbb{Q}}(\alpha)$, is

$$\text{tr}_{K/\mathbb{Q}}(\alpha) = \text{tr}\,(T_\alpha).$$

(b) The ***norm*** of α relative to $K/\mathbb{Q}$, denoted as $N_{K/\mathbb{Q}}(\alpha)$, is

$$N_{K/\mathbb{Q}}(\alpha) = \det\,(T_\alpha).$$

Note that $\text{tr}_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, since T_α is a $\mathbb{Q}$-linear operator (hence the entries of any matrix representation of T_α are rational).

Let $\alpha \in K$. Let β be a $\mathbb{Q}$-basis for K and let $A = [T_\alpha]_\beta$. Consider the characteristic and minimal polynomials $f, p \in \mathbb{Q}[x]$, respectively, of A. Notice that, for $g \in \mathbb{Q}[x]$ and $v \in K$,

$$g(T_\alpha)\,v = g(\alpha)\,v,$$

since $T_\alpha^m v = \alpha^m v$ for $m \in \mathbb{N} \cup \{0\}$. In particular,

$$g(\alpha) = 0 \iff g(T_\alpha) = 0,$$

so that p is the minimal polynomial for α over $\mathbb{Q}$. By the Cayley-Hamilton theorem, $p | f$. However,

$$\deg(f) = [K : \mathbb{Q}] = n.$$

We consider the following particular case.

Case 1. *Suppose*

$$K = \mathbb{Q}(\alpha).$$

On the other hand, since p is the minimal polynomial of α,

$$\deg(p) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K : \mathbb{Q}] = n.$$

Hence $p|f$, $\deg(f) = \deg(p)$, and f, p are monic, so that $f = p$.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of α (i.e. the roots of p in $\mathbb{C}$). But the roots of the characteristic polynomial of an operator are the eigenvalues (with multiplicity) and $f = p$, so that

$$\operatorname{tr}_{K/\mathbb{Q}}(\alpha) = \operatorname{tr}(T_\alpha) = \sum_{j=1}^{n} \alpha_j$$

and

$$N_{K/\mathbb{Q}}(\alpha) = \det(T_\alpha) = \prod_{j=1}^{n} \alpha_j.$$

Also note that

$$\sum_{j=1}^{n} \alpha_j = -\left[x^{n-1}\right] p$$

and

$$(-1)\left[x^0\right] p = (-1)^n p(0).$$

Recall from the field theory that the embeddings of $K = \mathbb{Q}(\alpha)$ in $\mathbb{C}$ are exactly given by $\sigma_j(\alpha) = \alpha_j$ for $j \in \{1, \ldots, n\}$. That is,

$$\operatorname{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{j=1}^{n} \alpha_j = \sum_{j=1}^{n} \sigma_j(\alpha)$$

and

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^{n} \alpha_j = \prod_{j=1}^{n} \sigma_j(\alpha).$$

(End of Case 1)

Apart from Case 1, we want to compute $\operatorname{tr}_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha)$ *in general*. To do so, we introduce the following lemma with a technical proof.

Lemma 1.9.

Suppose that K is a number field with $[K : \mathbb{Q}] = n$ and let $\alpha \in K$ with $[K : \mathbb{Q}(\alpha)] = m$. Consider

$$\begin{aligned} T_\alpha : K &\to K \\ x &\mapsto \alpha x \end{aligned}.$$

Let $f \in \mathbb{Q}[x]$ be the characteristic polynomial of T_α and let $p \in \mathbb{Q}[x]$ be the minimal polynomial for α. Then

$$f = p^m.$$

Note that we recover Case 1 when $m = 1$ (i.e. $K = \mathbb{Q}(\alpha)$).

Proof. Let

$$\beta = \{y_1, \ldots, y_d\}$$

be a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$ and let

$$\beta' = \{z_1, \ldots, z_m\}$$

be a $\mathbb{Q}(\alpha)$-basis for K. By the tower theorem, we have that

$$\{y_j z_k\}_{1\le j\le d, 1\le k\le m}$$

is a $\mathbb{Q}$-basis for K.

Let $A = [T_\alpha]_\beta \in \mathbb{Q}^{d\times d}$ (where we consider the restriction $T_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$). Recall from linear algebra that

$$\alpha y_j = T_\alpha(y_j) = \left(A\,[y_j]_\beta\right)^T \begin{bmatrix} y_1 & \cdots & y_d^T \end{bmatrix} = (Ae_j)^T \begin{bmatrix} y_1 & \cdots & y_d^T \end{bmatrix} = \sum_{k=1}^{d} a_{k,i} y_k,$$

where $A = [a_{k,i}]_{k,i=1}^d$. This implies

$$\alpha y_i z_j = \sum_{k=1}^{d} a_{ki} y_k z_j. \qquad [1.2]$$

Consider the ordered basis

$$\gamma = (y_1 z_1, \ldots, y_d z_1, y_1 z_2, \ldots, y_d z_2, \ldots, y_1 z_m, \ldots, y_d z_m).$$

Then [1.2] gives (exercise)

$$[T_\alpha]_\gamma = \begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix}.$$

Immediately,

$$f = \det(xI - A)^m = p^m,$$

where the last equality follows from Case 1.

QED

Consider the setting of Lemma 1.9. Observe that

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{tr}(T_\alpha) = \sum_j \lambda_j,$$

where λ_j's are the eigenvalues of T_α. But f is the characteristic polynomial for T_α and $f = p^m$, so that

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha) = m \sum_{j=1}^{\frac{m}{n}} \alpha_j.$$

Similarly,

$$N_{K/\mathbb{Q}}(\alpha) = \left(\alpha_1 \cdots \alpha_{\frac{n}{m}}\right)^m.$$

The embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ are determined by $\sigma_j(\alpha) = \alpha_j$ for $j \in \left\{1, \ldots, \frac{n}{m}\right\}$. By Assignment 1, each σ_j extends to exactly m embeddings of K in $\mathbb{C}$. If $\rho_1, \ldots, \rho_n$ are the embeddings of K in $\mathbb{C}$, them

$$\mathrm{tr}_{K/Q}(\alpha) = m \sum_{j=1}^{n} \sigma_j(\alpha) = \sum_{j=1}^{n} \rho_n(\alpha).$$

Similarly,

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{j=1}^{n} \rho_j(\alpha).$$

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $\alpha, \beta \in K, q \in \mathbb{Q}$. Then

$$\operatorname{tr}_{K/\mathbb{Q}}(q\alpha + \beta) = \sum_{j=1}^{n} \sigma_j(q\alpha + \beta) = q \sum_{j=1}^{n} \sigma_j(\alpha) + \sum_{j=1}^{n} \sigma_j(\beta) = q \operatorname{tr}_{K/\mathbb{Q}}(\alpha) + \operatorname{tr}_{K/\mathbb{Q}}(\beta).$$

That is, $\operatorname{tr}_{K/\mathbb{Q}}$ is a linear map.

On the other hand,

$$N_{K/\mathbb{Q}}(q\alpha\beta) = \prod_{j=1}^{n} \sigma_j(q\alpha\beta) = \prod_{j=1}^{n} q\sigma_j(\alpha)\sigma_j(\beta) = q^n N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta).$$

Now suppose $\alpha \in \mathcal{O}_K$. Then

$$\operatorname{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha).$$

If α is the root of a monic $f \in K[x]$, then so are $\sigma_j(\alpha)$'s, since the minimal polynomial for α divides f. Hence $\operatorname{tr}_{K/\mathbb{Q}}(\alpha) \in \mathcal{O}_K$. But the trace is always a rational number, so that

$$\operatorname{tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}.$$

In a similar manner,

$$N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}.$$

Example 1.12.

Consider $K = \mathbb{Q}\left(\sqrt{d}\right)$, where $d \in \mathbb{N}$ is squarefree and $d \neq 1$. Let

$$\alpha = a + b\sqrt{d}$$

for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then

$$\operatorname{tr}_{K/\mathbb{Q}}(\alpha) = \left(a + b\sqrt{d}\right) + \left(a - b\sqrt{d}\right) = 2a$$

and

$$N_{K/\mathbb{Q}}(\alpha) = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = a^2 - db^2.$$

Recall that $a^2 - db^2$ is frequently used in (elementary) ring theory! That is

$$a + b\sqrt{d} \text{ is a unit in } \mathbb{Q}\left(\sqrt{d}\right) \iff a^2 - db^2 = 1 \text{ or } a^2 - db^2 = -1.$$

We have the following generalization, left as an exercise.

Exercise 1.13.

Consider a number field K and let $R = \mathcal{O}_K$. Prove that for $\alpha \in R$,

$$\alpha \in R^\times \iff N_{K/\mathbb{Q}}(\alpha) = 1 \text{ or } N_{K/\mathbb{Q}}(\alpha) = -1.$$

This concludes every properties of trace and norm for the course. As a first application, we are going to prove that every $\mathcal{O}_K$ is a free $\mathbb{Z}$-module.

Here we prove a very powerful theorem with a cascade of useful corollaries. Fix

$$K \text{ a number field with } [K:\mathbb{Q}] = n.$$

Theorem 1.10.
$(\mathcal{O}_K, +) \cong \mathbb{Z}^n$.

Proof. Let $\{x_1, \ldots, x_n\}$ be a $\mathbb{Q}$-basis for K. By Assignment 1, we may assume each $x_j \in \mathcal{O}_K$. Let

$$\begin{aligned} \varphi : K &\to \mathbb{Q}^n \\ x &\mapsto (\operatorname{tr}(xx_1), \ldots, \operatorname{tr}(xx_n)), \end{aligned}$$

where tr is the shorthand for $\operatorname{tr}_{K/\mathbb{Q}}$.

Since tr is $\mathbb{Q}$-linear, so that φ is $\mathbb{Q}$-linear. Moreover, if for $x \in K$,

$$\varphi(x) = 0,$$

then

$$\operatorname{tr}(xx_j) = 0, \qquad \forall j \in \{1, \ldots, n\}.$$

But $\{x_1, \ldots, x_n\}$ is a $\mathbb{Q}$-basis for K, so that

$$\operatorname{tr}(xy) = 0, \qquad \forall y \in K. \tag{1.3}$$

For contradiction, suppose $x \neq 0$. Since $x \in K$ is nonzero and K is a field, we have $x^{-1} \in K$. But

$$\operatorname{tr}(xx^{-1}) = \operatorname{tr}(1) = \operatorname{tr}(I_{n\times n}) = n \neq 0.$$

This contradicts [1.3], so we conclude $x = 0$. Hence φ has trivial kernel, which means φ is a monomorphism of $\mathbb{Q}$-vector spaces.

Since we know that $\varphi(\alpha) \in \mathbb{Z}$ for $\alpha \in \mathcal{O}_K$, it follows that

$$\mathcal{O}_K \overset{\varphi}{\cong} \varphi(\mathcal{O}_K) \subseteq \mathbb{Z}^n.$$

That is, $\mathcal{O}_K$ isomorphic to a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$.

By Fact 1.7, it follows that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module with $\operatorname{rank}(\mathcal{O}_K) \leq n$, since $\mathbb{Z}$ is a PID. But we have a $\mathbb{Q}$-linearly independent, hence $\mathbb{Z}$-linearly independent, set $\{x_1, \ldots, x_n\}$ contained in $\mathcal{O}_K$, so that $\operatorname{rank}(\mathcal{O}_K) \geq n$. Thus we conclude

$$\operatorname{rank}(\mathcal{O}_K) = n$$

by Fact 1.8.

QED

Example 1.14. Warning Example

Consider $\{1, \sqrt{5}\} \subseteq \mathbb{Q}(\sqrt{5})$, which is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{5})$. However, it is not an *integral basis* for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$.

Theorem 1.10 only shows that *integral basis exists*, but it hasn't constructed one!

Corollary 1.10.1.
If I is a nonzero ideal of $\mathcal{O}_K$, then $(I, +) \cong \mathbb{Z}^n$.

Proof. Let $\{x_1, \ldots, x_n\}$ be an integral basis for $\mathcal{O}_K$ and let $a \in I$ be nonzero. Then $\{ax_1, \ldots, ax_n\}$ is a $\mathbb{Z}$-linearly independent subset of I, so that $n \leq \operatorname{rank}(I)$.

QED

Corollary 1.10.2.
If I is a nonzero ideal of $\mathcal{O}_K$, then $\mathcal{O}_K / I$ is finite.

To prove Corollary 1.10.2, here is the last fact we steal from commutative algebra.

Fact 1.11.

If M is a finitely generated $\mathbb{Z}$-module, then $M \cong \mathbb{Z}^n \times T$, where is T is a finite $\mathbb{Z}$-module.

Fact 1.11 is a consequence of the unfamous *structure theorem for finitely generated modules over a PID.*

Proof of Corollary 1.10.2

By Fact 1.11, we know

$$\mathcal{O}_K / I \cong Z^k \times T$$

as Z-modules, where T is finite. We are going to show that $k = 0$. To do so, observe that for $k \geq 1$, there is an element of infinite order in $\mathbb{Z}^k$. Hence it suffices to show that there is no element of infinite order in $\mathcal{O}_K / I$.

Suppose

$$\overline{x} = x + I \in \mathcal{O}_K / I$$

is an element of infinite order for contradiction. Let $\{x_1, \ldots, x_n\}$ be an integral basis for I. We note that, since $x_1, \ldots, x_n \in I$ but $x + I$ has infinite order, so that $x \notin I$.

Claim 1. *$\{x, x_1, \ldots, x_n\}$ is linearly independent.*

Suppose

$$cx + \sum_{j=1}^{n} c_j x_j = 0$$

for some $c, c_1, \ldots, c_n \in \mathbb{Z}$. Then

$$c\overline{x} = 0 + I.$$

But $\overline{x}$ has an infinite order, so that $c = 0$. But $x_1, \ldots, x_n$ are linearly independent, so that $c_1, \ldots, c_n = 0$ as well.

(End of Claim 1)

Note that the conclusing of Claim 1 contradicts the fact that $I \cong \mathbb{Z}^n$. Thus we conclude that

$$\mathcal{O}_K / I \cong T.$$

QED

Corollary 1.10.3.

Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Proof. Since P is a prime ideal, $\mathcal{O}_K / P$ is an integral domain. By Corollary 1.10.2, $\mathcal{O}_K / P$ is a finite integral domain, so it is a field. Hence P is maximal.

QED

Corollary 1.10.4.

$\mathcal{O}_K$ is Noetherian.

Proof. Let I be an ideal of $\mathcal{O}_K$. Then I is a free $\mathbb{Z}$-module with finite rank n, which means I is a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}$ is a submodule of $\mathcal{O}_K$, I is also a finitely generated $\mathcal{O}_K$.

QED

II. Discriminant

Suppose we have a number field K with $[K:\mathbb{Q}] = n$ and let $R = \mathcal{O}_K$. Given $\{v_1, \ldots, v_n\} \subseteq R$, we desire to find a way to *discriminate* whether or not $\{v_1, \ldots, v_n\}$ is an integral basis for R.

Fix K, R throughout.

1. Elementary Properties of Discriminant

We first record the definition of discriminant and than investigate many importnat properties of it.

Def'n 2.1. **Discriminant** of Finite Subset of K

Let $\sigma_1, \ldots, \sigma_n$ be embeddings of K in $\mathbb{C}$. The ***discriminant*** of $\{a_1, \ldots, a_n\} \subseteq K$, denoted as $\operatorname{disc}(a_1, \ldots, a_n)$, is

$$\operatorname{disc}(a_1, \ldots, a_n) = \det\left(\left[\sigma_i(a_j)\right]_{i,j=1}^n\right)^2.$$

Because of the presenece of the power 2, Def'n 2.1 is *independnet* of choice of ordering of the σ_i's and a_j's.

Consider

$$B = \left[\sigma_i(a_j)\right]_{i,j}^n$$

and let $A = B^T$. Since determinant is multiplicative and is invariant under transpose, it follows

$$\det(a_1, \ldots, a_n) = \det(AB).$$

However, the (i,j)th entry of AB is

$$\begin{bmatrix}\sigma_1(a_i) & \cdots & \sigma_n(a_i)\end{bmatrix}\begin{bmatrix}\sigma_1(a_j) \\ \vdots \\ \sigma_n(a_j)\end{bmatrix} = \sum_{k=1}^n \sigma_k(a_i)\sigma_k(a_j) = \sum_{k=1}^n \sigma_k(a_ia_j) = \operatorname{tr}_{K/\mathbb{Q}}(a_ia_j).$$

Therefore,

$$\operatorname{disc}(a_1, \ldots, a_n) = \det\left[\operatorname{tr}_{K/\mathbb{Q}}(a_ia_j)\right]_{i,j=1}^n.$$

Some texts use the above formula as the definition.

Since we know that $\operatorname{tr}_{K/\mathbb{Q}}(a)$ is a rational number for $a \in K$,

$$\operatorname{disc}(a_1, \ldots, a_n) \in \mathbb{Q}.$$

In particular, when $a_1, \ldots, a_n \in \mathcal{O}_K$,

$$\operatorname{disc}(a_1, \ldots, a_n) \in \mathbb{Z}.$$

Consider $v, w \in K^n$ and $A \in \mathbb{Q}^{n\times n}$ such that

$$Av = w.$$

Then, for $i \in \{1, \ldots, n\}$,

$$A\sigma_i(v) = \begin{bmatrix}A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{n,1} & \cdots & A_{n,n}\end{bmatrix}\begin{bmatrix}\sigma_i(v_1) \\ \vdots \\ \sigma_i(v_n)\end{bmatrix} = \begin{bmatrix}\sigma_i\left(\sum_{j=1}^n A_{1,j}v_j\right) \\ \vdots \\ \sigma_i\left(\sum_{j=1}^n A_{n,j}v_j\right)\end{bmatrix} = \begin{bmatrix}\sigma_i(w_1) \\ \vdots \\ \sigma_i(w_n)\end{bmatrix}.$$

Therefore,
$$A\left[\sigma_i\left(v_j\right)\right]_{i,j=1}^n=\left[\sigma_i\left(w_j\right)\right]_{i,j=1}^n.$$
Thus we conclude
$$\det\left(A^2\right)\operatorname{disc}(v)=\operatorname{disc}(w).$$

Let $\{v_1,\dots,v_n\}\subseteq\mathcal{O}_K$ be an integral basis for $\mathcal{O}_K$ and let $\{w_1,\dots,w_n\}\subseteq\mathcal{O}_K$. Then there is $\left\{C_{i,j}\right\}_{i,j}^n\subseteq\mathbb{Z}$ such that
$$w_i=\sum_{j=1}^n C_{i,j}v_j,\qquad\qquad \forall i\in\{1,\dots,n\}.$$
That is,
$$w=Cv,$$
where $C=\left[C_{i,j}\right]_{i,j=1}^n$. Hence
$$\operatorname{disc}(w)=\det\left(C^2\right)\operatorname{disc}(v).$$
Let $\beta=\{v_1,\dots,v_n\}$ and
$$\begin{aligned}T:\mathcal{O}_K&\to\mathcal{O}_K\\ v_i&\mapsto w_i,\qquad\qquad \forall i\in\{1,\dots,n\}\end{aligned},$$
which is a $\mathbb{Z}$-linear homomorphism. Then
$$[T]_\beta=\begin{bmatrix}[T(v_1)]_\beta & \cdots & [T(v_n)]_\beta\end{bmatrix}=\begin{bmatrix}[w_1]_\beta & \cdots & [w_n]_\beta\end{bmatrix}=C^T.$$

Let $A\in\mathbb{Z}^{n\times n}$. If $\det(A)\neq 0$, then recall that
$$A^{-1}=\frac{1}{\det(A)}\operatorname{adj}(A).$$
Since $A\in\mathbb{Z}^{n\times n}$, every cofactor of A is in $\mathbb{Z}$, so that $\operatorname{adj}(A)\in\mathbb{Z}^{n\times n}$. Thus,
$$A^{-1}\in\mathbb{Z}^{n\times n}\iff\det(A)=1\text{ or }\det(A)=-1.$$

Let $\{v_1,\dots,v_n\}\ \mathcal{O}_K$ be an integral basis and suppose
$$\operatorname{disc}(v)=\operatorname{disc}(w)$$
for some $\{w_1,\dots,w_n\}\in\mathcal{O}_K$. Then
$$Cv=w$$
for some $C\in\mathbb{Z}^{n\times n}$. This implies that
$$\det\left(C^2\right)\operatorname{disc}(v)=\operatorname{disc}(w),$$
so that
$$(\det(C))^2=1.^2$$
Hence $\det(C)=1$ or $\det(C)=-1$, which means C is invertible with $C^{-1}\in\mathbb{Z}^{n\times n}$. This implies that C^T is invertible with integer inverse, so that
$$T:\mathcal{O}_K\to\mathcal{O}_K$$

[2] Note the degenerate case where $\operatorname{disc}(v)=\operatorname{disc}(w)=0$. We will show that this never happens.

Therefore, given an integral basis $\{v_1, \ldots, v_n\}$, we can search for other integral basis by looking at subsets $\{w_1, \ldots, w_n\}$ whose discriminant agrees with $\operatorname{disc}(v)$.

Conversely, if

$$\{v_1, \ldots, v_n\}, \{w_1, \ldots, w_n\} \subseteq \mathcal{O}_K$$

are integral bases, then $Av = w, Bw = v$ for some $A, B \in \mathbb{Z}^{n\times n}$. It follows that $\det(A)^2 \operatorname{disc}(v) = \operatorname{disc}(w)$ and $\det(B)^2 \operatorname{disc}(w) = \operatorname{disc}(v)$. Thus we have that

$$\operatorname{disc}(v) = \operatorname{disc}(w).$$

Let $\{a_1, \ldots, a_n\} \subseteq K$. Suppose there is nonzero $(c_1, \ldots, c_n) \in \mathbb{Q}^n$ such that

$$\sum_{j=1}^{n} c_j a_j = 0.$$

This means

$$\sum_{j=1}^{n} c_j \sigma_i\left(a_j\right) = 0$$

for any embedding σ_i of K in $\mathbb{C}$, so that $\left[\sigma_i\left(a_j\right)\right]_{i,j}^{n}$ is not invertible. It follows that

$$\operatorname{disc}(a_1, \ldots, a_n) = 0.$$

Conversely, suppose that $\operatorname{disc}(a_1, \ldots, a_n) = 0$. Then the columns of $\left[\sigma_i\left(a_j\right)\right]_{i,j=1}^{n}$ are linearly dependent. That is,

$$\sum_{j=1}^{n} c_j \sigma_i\left(a_j\right) = 0, \qquad \forall i,$$

for some nonzero $(c_1, \ldots, c_n) \in \mathbb{Q}^n$. By considering $\sigma_i = \iota : K \to \mathbb{C}$ by $k \mapsto k$, we observe that $\sum_{j=1}^{n} a_j = 0$. Thus $\{a_1, \ldots, a_n\}$ is $\mathbb{Q}$-linearly dependent.

2. Discriminant of Number Fields

Fix a number field K with $[K : \mathbb{Q}] = n$.

Def'n 2.2. **Discriminant** of a Number Field
We define the ***discriminant*** of K, $\operatorname{disc}(K)$, as

$$\operatorname{disc}(K) = \operatorname{disc}(v_1, \ldots, v_n),$$

where $v_1, \ldots, v_n$ is an integral basis for $\mathcal{O}_K$.

Example 2.1.
Consider $K = \mathbb{Q}\left(\sqrt{d}\right)$, where $d \neq 1$ is squarefree.

Case 1. $d \equiv 1 \bmod 4$.
We claim that $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis (check this; exercise!). Then

$$\operatorname{disc}(K) = \det\begin{bmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{bmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 = \left(-\sqrt{d}\right)^2 = d.$$

(End of Case 1)

Case 2. $d \equiv 2, 3 \mod 4$.

In this case, $\left\{1, \sqrt{d}\right\}$ is an integral basis, so that

$$\operatorname{disc}(K) = \det \begin{bmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{bmatrix}^2 = 4d.$$

(End of Case 2)

---

3. Computational Considerations

Recall 2.3. **Discriminant** of a Polynomial

Let $p \in \mathbb{C}[x]$ and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the roots of p. Then we define the *discriminant* of p, $\operatorname{disc}(p)$, by

$$\operatorname{disc}(p) = \prod_{i<j} \left(\alpha_i - \alpha_j\right)^2.$$

Example 2.2. Discriminant of Quadratic, Cubic Polynomials

For a quadratic $x^2 + bx + c$,

$$\operatorname{disc}\left(x^2 + bx + c\right) = b^2 - 4c.$$

For a *depressed* cubic $x^3 + bx + c$,

$$\operatorname{disc}\left(x^3 + bx + c\right) = -4b^3 - 27c^2.$$

To turn a general cubic $x^3 + ax^2 + bx + c$ into a depressed cubic, substitute x by $x - \frac{a}{3}$ which *eliminates* x^2 term. Since every root is *shifted by the same amout* $\frac{a}{3}$, it follows that the discriminant is the same:

$$\operatorname{disc}\left(x^3 + ax^2 + bx + c\right) = -4b^3 - 27c^2.$$

Def'n 2.4. **Discriminant** of an Algebraic Number

Suppose $\alpha \in \mathbb{C}$ is such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Then we define the ***discriminant*** of α, $\operatorname{disc}(\alpha)$, to be

$$\operatorname{disc}(\alpha) = \operatorname{disc}\left(1, \alpha, \ldots, \alpha^{n-1}\right).$$

Observe that $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ is an integral basis for $\mathbb{Z}[\alpha]$. Moreover,

$$\operatorname{disc}(\alpha) = \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}^2.$$

Observe that we have a Vandermonde matrix, whose determinant is famously

$$\det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix} = \prod_{i<j} \left(\alpha_i - \alpha_j\right)$$

Since we have the square term, it follows that

$$\operatorname{disc}(\alpha) = \prod_{i<j} \left(\alpha_i - \alpha_j\right)^2 = \operatorname{disc}(p),$$

where p is the minimal polynomial of α. Thus the discriminant of an algebraic number and its minimal polynomial coincides.

Suppose $\{v_1, \ldots, v_n\}$ is an integral basis for $\mathcal{O}_{\mathbb{Q}(\alpha)}$. Then

$$\begin{bmatrix} 1 \\ \cdots \\ \alpha^{n-1} \end{bmatrix} = A \begin{bmatrix} v_1 \\ \cdots \\ v_n \end{bmatrix}$$

for some invertible $A \in \mathbb{Z}^{n \times n}$. Therefore,

$$\operatorname{disc}(\alpha) = \det(A)^2 \operatorname{disc}(\mathbb{Q}(\alpha)) = \left[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]\right]^2 \operatorname{disc}(\mathbb{Q}(\alpha))$$

by Assignment 2.

As a corollary, if $\operatorname{disc}(\alpha)$ is squarefree, then

$$\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha].$$

Example 2.3.

Suppose $\alpha \in \mathbb{C}$ is such that $p(\alpha) = 0$, where

$$p = x^3 + x + 1.$$

Note that p is irreducible over $\mathbb{Q}$, so it is the minimal polynomial for α. Then $\operatorname{disc}(\alpha) = \operatorname{disc}(p) = -4 - 27 = -31$, which is prime so is squarefree.

Thus

$$\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha] = \left\{a + b\alpha + c\alpha^2\right\}.$$

Let α be an algebraic number with minimal polynomial $p \in \mathbb{Q}[x]$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Let $\alpha_1 = \alpha$ and let $\alpha_2, \ldots, \alpha_n$ be the conjugates of α. Then

$$p = (x - \alpha_1) \cdots (x - \alpha_n).$$

Consider the *formal derivative* of p, which we can find using the product rule:

$$p' = \sum_{i=1}^{n} \prod_{j=1, j\neq i}^{n} \left(x - \alpha_j\right).$$

Then

$$p'(\alpha_i) = \prod_{j=1, j\neq i}^{n} \left(\alpha_i - \alpha_j\right), \qquad \forall i.$$

Now, given the embeddings $\sigma_1, \ldots, \sigma_n : \mathbb{Q}(\alpha) \to \mathbb{C}$,

$$\begin{aligned} N_{K/\mathbb{Q}}\left(p'(\alpha)\right) &= \prod_{i=1}^{n} \sigma_r\left(p'(\alpha)\right) = \prod_{i=1}^{n} p'(\sigma_i(\alpha)) && \text{since } \sigma_i \text{ fix each element in } \mathbb{Q} \\ &= \prod_{i=1}^{n} p'(\alpha_i) = \prod_{i\neq j}^{n} \left(\alpha_i - \alpha_j\right) = (-1)^{\binom{n}{2}} \prod_{i<j}^{n} \left(\alpha_i - \alpha_j\right)^2 \\ &= (-1)^{\binom{n}{2}} \operatorname{disc}(p) = (-1)^{\binom{n}{2}} \operatorname{disc}(\alpha). \end{aligned}$$

Def'n 2.5. **Resultant**

Let $f = \sum_{i=0}^{n} a_i x^i, g = \sum_{j=0}^{m} b_j x^j \in \mathbb{C}[x]$. Then we define the ***resultant*** of f, g, denoted as $\operatorname{res}(f, g)$, is the determinant of

$$\begin{bmatrix} a & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a & 0 & \cdots & \cdots & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a & 0 & \cdots & 0 \\ b & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & b & 0 & \cdots & \cdots & \cdots & 0 \\ & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b & 0 & \cdots & 0 \end{bmatrix} \in \mathbb{Q}^{(n+m)\times(n+m)},$$

where $a = (a_n, \ldots, a_0), b = (b_m, \ldots, b_0)$.

Example 2.4.

We have

$$\operatorname{res}\left(x^3 + x + 2, x^2 + 4x - 1\right) = \det \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 1 & 2 \\ 1 & 4 & -1 & 0 & 0 \\ 0 & 1 & 4 & -1 & 0 \\ 0 & 0 & 1 & 4 & -1 \end{bmatrix}.$$

Fact 2.1.

Let $\alpha \in \mathbb{C}$ be an algebraic number with the minimal polynomial $p \in \mathbb{Q}[x]$ such that $\alpha \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Then

$$\operatorname{disc}(\alpha) = (-1)^{\binom{n}{2}} \operatorname{res}\left(p, p'\right).$$

Example 2.5.

Let $\alpha \in \mathbb{C}$ be such that $p(\alpha) = 0$, where

$$p = x^3 - x^2 - 1.$$

Since $p(1), p(-1) \neq 0$, so p is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Note that

$$p' = 3x^2 - 2x.$$

It follows that

$$\operatorname{disc}(\alpha) = (-1)^{\binom{3}{2}} \det \begin{bmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 & -1 \\ 3 & -2 & 0 & 0 & 0 \\ 0 & 3 & -2 & 0 & 0 \\ 0 & 0 & 3 & -2 & 0 \end{bmatrix} = 31.$$

Since 31 is squarefree, so that

$$\mathcal{O}_K = \mathbb{Z}[\alpha].$$

III. Prime Factorization

Let K be a number field and let $R = \mathcal{O}_K$. Let's recall some important properties of R as a ring.

(a) Every nonzero prime ideal of R is maximal.

(b) If I is a nonzero ideal, then R/I is finite.

(c) R is Noetherian.

1. Some Useful Ring Theory

Proposition 3.1.

Let R be a ring.[1] The following are equivalent.

(a) R is Noetherian.

(b) Every ascending chain of ideals stabilizes.[2] *ascending chain condition (acc)*

(c) Every nonempty collection of ideals of R has a maximal (with respect to inclusion) element.

[1] Let us recall that a ring is always commutative and unital in our course.
[2] This is the *usual* definition of Noetherian ring in commutative algebra.

Proof is left as an exercise

The idea for (b) $\implies$ (a) is that, given an ascending chain of ideals, the union is also an ideal. For this ideal to be finitely generated, it must be the case that the chain stabilizes.

For (b) $\implies$ (c), if we assume (c) is false, then we can construct an ascending chain of ideals that does not stabilize.

Proposition 3.2.

Let R be a Noetherian ring and let I be a proper ideal of R. Then there exists prime ideals $P_1, \ldots, P_n$ of R such that

(a) $I \subseteq P_i$ for i;

(b) $P_1 \cdots P_n \subseteq I$.

We know that prime factorization of numbers does not work well in a ring of integers. After all, a ring of integers need not be a UFD! Hence, instead of factoring numbers, we are going to *factor ideals* in $\mathcal{O}_K$. This will work well, and introduce us the notion of *Dedekind domains*.

Note that Proposition 3.2 is bit more general than we require, that it works for any *Noetherian ring*. Indeed, any ring of integer is a Noetherian ring (Corollary 1.10.4, *the* result of Chapter 1).

Proof of Proposition 3.2

Let X be the collection of proper ideals of R not having the property. Assume for contradiction that X is nonempty. Let $I \in X$ be an maximal *element* of X (we do not insist that I is a maximal *ideal* in R).

Clearly I is not prime. If not, then take $P_1 = I$ and observe that I has the property. Since I is not prime, we may find $a, b \in R$ such that $ab \in I$ but $a, b \notin I$. By maximality of I, $I + \langle a \rangle, I + \langle b \rangle \notin X$. Note that, for any ideal J, $IJ \subseteq I$ (this is a property of ideal product; check this!). Moreover, $ab \in I$ and $\langle a \rangle, \langle b \rangle$ are principal ideals, so that $\langle a \rangle \langle b \rangle = \langle ab \rangle \subseteq I$. Hence it follows that

$$(I + \langle a \rangle)(I + \langle b \rangle) \subseteq I.$$

Hence $I + \langle a \rangle, I + \langle b \rangle \neq R$ (since $JR = RJ = J$ for any ideal J). Therefore, there are prime ideals $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ such that

(a) $I + \langle a \rangle \subseteq P_i, I + \langle b \rangle \subseteq Q_j$ for $i, j \implies I \subseteq I + \langle a \rangle \subseteq P_i, I \subseteq I + \langle b \rangle \subseteq Q_j$ for i, j; and

(b) $P_1 \cdots P_n \subseteq I + \langle a \rangle, Q_1 \cdots Q_m \subseteq I + \langle b \rangle \implies P_1 \cdots P_n Q_1 \cdots Q_m \subseteq (I + \langle a \rangle)(I + \langle b \rangle) \subseteq I$.

Thus $I \notin X$, which is a contradiction.

QED

Def'n 3.1. **Coprime** Ideal
Let R be a ring and let $I, J \subseteq R$ be prime ideals. We say I, J are ***coprime*** if and only if $I + J = R$.

A motivation for the above definition comes from the Bezout lemma.

Proposition 3.3.
Let R be a ring and let I, J be coprime ideals of R. Then for any $n, m \in \mathbb{N}$, I^n, J^m are coprime.

Proof. Since I, J are proper, so are $I^n \subseteq I, J^m \subseteq J$. Suppose for contradiction that

$$I^n + J^m \neq R.$$

Then $I^n + J^m \subseteq M$ for some maximal ideal M, which means $I^n, J^m \subseteq M$. But any maximal ideal is a prime ideal, so that M is a prime ideal. Recall that,

given two ideals $\tilde{I}, \tilde{J}$ and a prime ideal P such that $\tilde{I}, \tilde{J} \subseteq P$, $\tilde{I} \subseteq P$ or $\tilde{J} \subseteq P$.

In particular, $I, J \subseteq M$. This means $I + J \subseteq M \neq R$, a contradiction.

QED

Recall the following theorem from ring theory.

Theorem 3.4. Chinese Remainder Theorem
Let R be a ring and let I, J be coprime ideals of R. Then $R/IJ \cong R/I \times R/J$.

Proof. When we want two algebraic objects to be *isomorphic*, 99.9% of the time we want to explicitly find an isomorphism. Since we are working with quotient rings, we resort to the first isomorphism theorem.

Let

$$\begin{aligned} \varphi : R &\to R/I \times R/J \\ x &\mapsto (x + I, x + J). \end{aligned}$$

Then

$$\ker(\varphi) = I \cap J.$$

Now observe that,

$$IJ \subseteq I \cap J = (I \cap J) R = (I \cap J)(I + J) = \underbrace{(I \cap J) I}_{\subseteq IJ} + \underbrace{(I \cap J) J}_{\subseteq IJ} \subseteq IJ,$$ [1]

so that

$$IJ \subseteq I.$$

Hence we conclude

$$\ker(\varphi) = IJ.$$

To invoke the first isomorphism theorem, we want to show that φ is surjective. Take $a \in I, b \in J$ such that $a + b = 1$ (since $I + J = R$). For $x, y \in R$

$$\begin{aligned} \varphi(ax + by) &= \left(\underbrace{ax}_{\in I} + by + I, ax + \underbrace{by}_{\in J} + J \right) = (by + I, ax + J) \\ &= (b + I, a + J)(y + I, x + J) = (1 + I, 1 + J)(y + I, x + J) = (y + I, x + J). \end{aligned}$$

Note that we are using $a + b = 1$ but $a + I = 0 + I, b + J = 0 + J$ to obtain the second-last equality.

Thus φ is surjective and

$$R/IJ \cong R/I \times R/J$$

by the first isomorphism theorem.

[1] Note that the above argument worked because of the *coprimeness* of I, J: $R = I + J$.

QED

Theorem 3.5. Generalized Chinese Remainder Theorem

Let R be a ring and let $I_1, \dots, I_n$ be *pairwise* coprime ideals. Then $R/I_1 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n$.

Proposition 3.6.

Let R be a finite ring. Then

$$R \cong R/P_1^{n_1} \times \cdots \times R/P_m^{n_m}$$

for some distinct prime ideals $P_1, \dots, P_m$ and $n_1, \dots, n_m \in \mathbb{N}$.

In case R is an integral domain, we can simply take $P_1 = \{0\}$ and *call it a day!* In fact, the key idea for the general case is to identify R with $R/\{0\}$.

Proof of Proposition 3.6

Note that

$$R \text{ is finite} \implies R \text{ is Noetherian.}^1$$

So we may find prime ideals $Q_1, \dots, Q_k \subseteq R$ such that $Q_1 \cdots Q_k = \{0\}$. *Graping* the Q_i's we obtain distinct prime ideals $P_1, \dots, P_m$ such that

$$P_1^{n_1} \cdots P_m^{n_m} = \{0\}.$$

For each P_i,

$$R \text{ is finite and } P_i \text{ is prime} \implies R/P_i \text{ is finite integral domain} \implies R/P_i \text{ is a field.}$$

Hence each P_i is maximal, which imply

$$P_i + P_j = R, \qquad \forall i \neq j.$$

It follows $P_i^{n_i} + P_j^{n_j} = R$. Hence $P_1, \dots, P_m$ are pairwise coprime ideals, so by the generalized Chinese remainder theorem,

$$R \cong R/\{0\} = R/P_1^{n_1} \cdots P_m^{n_m} \cong R/P_1^{n_1} \times \cdots R/P_m^{n_m}.$$

[1] "Good luck in finding an infinite ascending chain in a finite ring!" - Blake

QED

2. Prime Ideals of a Ring of Integers

Once again, let K be a number field of degree n and let $R = \mathcal{O}_K$. Then we recall that

(a) R is Noetherian;

(b) R/I is finite for any nonzero proper ideal I;

(c) every ideal $\bar{J}$ of R/I is of the form $\bar{J} = J/I$, where $J \subseteq R$ is an ideal such that $I \subseteq J$; moreover, $\bar{J}$ is prime if and only if J is prime;[3] and *correspondence theorem*

(d) $R/I \cong (R/I)\,/\,(P_1^{n_1}/I) \times \cdots \times (R/I)\,/\,(P_m^{n_m}/I) \cong R/P^{n_1} \times \cdots \times R/P_m^{n_m}$, where each $P_i \subseteq R$ is prime with $I \subseteq P_i$.

The big idea for this section is that:

to understand I, we study the prime ideals P containing I.

Turns out, for a prime ideal P,

$$I \subseteq P \iff P \text{ is a } \textit{prime factor} \text{ of } I.$$

[3] In fact, this is true for any ring!