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

$$\alpha^2 = \alpha + 1. \qquad [1.1]$$

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*.

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
$(\impliedby)$ This direction is trivial, as any minimal polynomial is monic.

$(\implies)$ 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 $m \in \mathbb{Z}[x]$.

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 $N = \max_{1 \leq j \leq n} \deg(f_j)$. 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 $\deg\left(x^{N+1}\right) = N + 1 > N = \max_{1 \leq j \leq n} \deg(f_j)$, 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
$$\mathbb{Z}[\alpha] = \sum_{j=1}^{n} \mathbb{Z}\,\alpha_j, \qquad \mathbb{Z}[\beta] = \sum_{j=1}^{m} \mathbb{Z}\,\beta_j.$$
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

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

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

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

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

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

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

Let N be an R-submodule of M. Consider

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

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

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

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

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

for some $r_1, \ldots, r_q \in R$. 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 $s_1, \ldots, s_p \in R$.

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.

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 $\operatorname{rank}(M) = n < \infty$.

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

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

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

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 $\operatorname{tr}_{K/\mathbb{Q}}(\alpha)$, is

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

(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 $\operatorname{tr}_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, 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

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

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

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

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

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

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

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

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

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

Consider the ordered basis

$$\gamma = \left(y_1 z_1, \dots, y_d z_1, y_1 z_2, \dots, y_d z_2, \dots, y_1 z_m, \dots, y_d z_m\right).$$

Then [1.2] gives (exercise)

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

Immediately,

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

where the last equality follows from Case 1.

QED

Consider the setting of Lemma 1.9. Observe that

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

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 $j \in \left\{1, \dots, \frac{n}{m}\right\}$. By Assignment 1, each σ_j extends to exactly m embeddings of K in $\mathbb{C}$. If $\rho_1, \dots, \rho_n$ are the embeddings of K in $\mathbb{C}$, them

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

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

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

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

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

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

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

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

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

Therefore,

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

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 $\{v_1,\ldots,v_n\} \subseteq \mathcal{O}_K$ be an integral basis for $\mathcal{O}_K$ and let $\{w_1,\ldots,w_n\} \subseteq \mathcal{O}_K$. Then there is $\left\{C_{i,j}\right\}_{i,j}^n \subseteq \mathbb{Z}$ such that

$$w_i = \sum_{j=1}^n C_{i,j}v_j, \qquad \forall i \in \{1,\ldots,n\}.$$

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 $\beta = \{v_1,\ldots,v_n\}$ and

$$\begin{aligned} T : \mathcal{O}_K &\to \mathcal{O}_K \\ v_i &\mapsto w_i, \qquad \forall i \in \{1,\ldots,n\}' \end{aligned}$$

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 $\{v_1,\ldots,v_n\}\,\mathcal{O}_K$ be an integral basis and suppose

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

for some $\{w_1,\ldots,w_n\} \in \mathcal{O}_K$. 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

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

for any embedding σ_i of K in $\mathbb{C}$, so that $[\sigma_i(a_j)]_{i,j}^n$ 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 $[\sigma_i(a_j)]_{i,j=1}^n$ are linearly dependent. That is,

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

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** of Polynomials

Let $f=\sum_{i=0}^{n}a_ix^i, g=\sum_{j=0}^{m}b_jx^j\in\mathbb{C}[x]$. 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. A Glimpse of Prime Factorization

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.

Def'n 3.1. **Coprime** Ideals
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 find an isomorphism.*" - Blake

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 $I_1, \ldots, I_n$ 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 $P_1, \ldots, P_m$ and $n_1, \ldots, n_m \in \mathbb{N}$.

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

2. Prime Ideals of a Ring of Integers

Recall.

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

(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.[1] *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 $I \subseteq P_i$.

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

Here are some bing ideas for this section:

(a) To understand I, we study the prime ideals P containing I. Turns out, for a prime ideal P,

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

(b) The prime ideals of R/I are P/I, where P is a prime ideal containing I.

(c) Say P is a prime ideal containing I. Then $|R/P| = p^m$ for some prime p and $m \in \mathbb{N}$. Now,

$$p^m + P = p^m (1 + P) = 0 + P$$

by Lagrange's theorem, which imply that $p^m \in P$. Since P is a prime ideal, it follows $p \in P$. Hence we have

$$\langle p \rangle \subseteq P.$$

That is, any prime ideal containing I also contains a principal ideal generated by *an old-school prime number*. Because of this, we first search for ideals of the form $\langle p \rangle$ to find candidates for prime factorization of I.

Example 3.1.
Let $K = \mathbb{Q}\left(\sqrt{2}\right), R = \mathcal{O}_K = \mathbb{Z}\left[\sqrt{2}\right]$. Find all prime ideals P of R containing $\langle 5 \rangle$.

Answer. Observe that

$$R/\langle 5 \rangle = \mathbb{Z}\left[\sqrt{2}\right] / \langle 5 \rangle \cong \mathbb{Z}[x] / \left\langle x^2 - 2, 5 \right\rangle = \mathbb{Z}[x] / \left\langle 5, x^2 - 2 \right\rangle \cong \mathbb{Z}_5[x] / \left\langle x^2 - 2 \right\rangle.$$

But $x^2 - 2$ is irreducible over $\mathbb{Z}_5$, which means $\left\langle x^2 - 2 \right\rangle$ is a maximal ideal of $\mathbb{Z}_5[x]$. Therefore, $\mathbb{Z}_5[x] / \left\langle x^2 - 2 \right\rangle$ is a field, and so is $R/\langle 5 \rangle$. Hence $\langle 5 \rangle$ is a maximal ideal of R, which means the only prime ideal containing $\langle 5 \rangle$ is $\langle 5 \rangle$ itself.

QED

Example 3.2.
Let $K = \mathbb{Q}\left(\sqrt{2}\right), R = \mathcal{O}_K = \mathbb{Z}\left[\sqrt{2}\right]$. Find all prime ideals P of R containing $\langle 7 \rangle$.

Answer. Observe

$$R/\langle 7 \rangle = \mathbb{Z}[x] / \left\langle x^2 - 2, 7 \right\rangle = \mathbb{Z}_7[x] / \left\langle x^2 - 2 \right\rangle.$$

But $x^2 - 2$ is reducible over $\mathbb{Z}_7$, namely

$$x^2 - 2 = (x+3)(x+4).$$

It follows $\left\langle x^2 - 2 \right\rangle = \langle x+3 \rangle \langle x+4 \rangle$, and the two ideals $\langle x+3 \rangle, \langle x+4 \rangle$ are coprime. It follows by the Chinese remainder theorem that

$$\mathbb{Z}_7[x] / \left\langle x^2 - 2 \right\rangle \cong \mathbb{Z}_7[x] / \langle x+3 \rangle \times \mathbb{Z}_7[x] / \langle x+4 \rangle \cong \mathbb{Z}_7 \times \mathbb{Z}_7, \tag{3.1}$$

where the last isomorphism is due to the first isomorphism theorem (or, we can intuitively think that we can replace x by $-3, -4$ and retain every element of $\mathbb{Z}_7$ from $\mathbb{Z}_7[x]$, respectively).

The prime ideals of $\mathbb{Z}_7 \times \mathbb{Z}_7$ are

$$P_1 = \langle (1,0) \rangle, P_2 = \langle (0,1) \rangle.$$

Now, given an isomorphism φ, $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$. Hence we have to *undo* isomorphisms in [3.1] with elements $(1,0), (0,1)$ to figure out the prime ideals containing $\langle 7 \rangle$:

$$\begin{aligned}
(1,0) &\mapsto (1 + \langle x+3 \rangle, 0 + \langle x+4 \rangle) \\
&\mapsto x + 4 + \left\langle x^2 - 2 \right\rangle && \text{since } x+4 \text{ is 1 modulo } x+3 \text{ and 0 modulo } x+4 \\
&\mapsto x + 4 + \left\langle x^2 - 2, 7 \right\rangle \\
&\mapsto \sqrt{2} + 4 + \langle 7 \rangle
\end{aligned}$$

and

$$(0,1) \mapsto (0 + \langle x+3 \rangle, 1 + \langle x+4 \rangle) \mapsto (-x-3) + \left\langle x^2 - 2 \right\rangle \mapsto -x - 3 + \left\langle x^2, 7 \right\rangle \mapsto -\sqrt{2} - 3 + \langle 7 \rangle.$$

Therefore, the prime ideals in R containing 7 are $Q_1 = \left\langle \sqrt{2} + 4, 7 \right\rangle, Q_2 = \left\langle -\sqrt{2} - 3, 7 \right\rangle$. Note that we are including 7 in each ideal in addition to $\sqrt{2} + 4, -\sqrt{2} - 3$, respectively, in order to mod out by $\langle 7 \rangle$. In fact, $\left\langle -\sqrt{2} - 3, 7 \right\rangle = \left\langle \sqrt{2} + 3, 7 \right\rangle$ and $\left(\sqrt{2} + 3\right)\left(\sqrt{2} - 3\right) = -7$, so that $Q_2 = \left\langle \sqrt{2} + 3 \right\rangle$.

Note that $\left(\sqrt{2} + 3\right)\left(\sqrt{4}\right) = 14 + 7\sqrt{2} \in \langle 7 \rangle$, so that $Q_1 Q_2 = \langle 7 \rangle$. That is, we factored $\langle 7 \rangle$ into prime ideals!

QED

Example 3.3.

Let $K = \mathbb{Q}\left(\sqrt{2}\right), R = \mathcal{O}_K = \left[\sqrt{2}\right]$. Find all prime ideals P of R containing $\langle 2 \rangle$.

Answer. We have

$$R/\langle 2 \rangle \cong \mathbb{Z}[x] / \left\langle x^2 - 2, 2 \right\rangle \cong \mathbb{Z}_2[x] / \left\langle x^2 - 2 \right\rangle = \mathbb{Z}_2[x] / \left\langle x^2 \right\rangle,$$

since $x^2 - 2 \equiv x^2 \mod 2$. Since $\mathbb{Z}_2[x] / \left\langle x^2 \right\rangle$ is very small,

$$\mathbb{Z}_2[x] / \left\langle x^2 \right\rangle = \left\{ 0 + \left\langle x^2 \right\rangle, 1 + \left\langle x^2 \right\rangle, x + \left\langle x^2 \right\rangle, x + 1 + \left\langle x^2 \right\rangle \right\},$$

given an ideal of $\mathbb{Z}_2[x] / \left\langle x^2 \right\rangle$, we can explicitly write down the elements.

Let P be a prime ideal of $\mathbb{Z}_2[x] / \left\langle x^2 \right\rangle$. Since P is an ideal, $0 + \left\langle x^2 \right\rangle \in P$. Since P is prime so proper, $1 + \left\langle x^2 \right\rangle \notin P$. Also,

$$\left(x + 1 + \left\langle x^2 \right\rangle\right)^2 = \left(x^2 + 2x + 1 + \left\langle x^2 \right\rangle\right) = 1 + \left\langle x^2 \right\rangle \notin P,$$

so that $x + 1 + \left\langle x^2 \right\rangle \notin P$, since P is prime. Hence $P = \left\langle 0 + \left\langle x^2 \right\rangle \right\rangle$ or $P = \left\langle x + \left\langle x^2 \right\rangle \right\rangle$. But $\mathbb{Z}_2[x] / \left\langle x^2 \right\rangle$ is not an integral domain, since $x + \left\langle x^2 \right\rangle$ is a zero divisor. It follows that

$$P = \left\langle x + \left\langle x^2 \right\rangle \right\rangle.$$

Retracing the isomorphisms,

$$x + \left\langle x^2 \right\rangle \mapsto x + \left\langle x^2 - 2, 2 \right\rangle \mapsto \sqrt{2} + \langle 2 \rangle.$$

Hence the only prime $Q \subseteq R$ with $2 \in Q$ is

$$Q = \left\langle \sqrt{2}, 2 \right\rangle = \left\langle \sqrt{2} \right\rangle.$$

Note that

$$\langle 2 \rangle = \left\langle \sqrt{2} \right\rangle^2.$$

Hence we have a prime factorization of $\langle 2 \rangle$ with *multiplicity*.

QED

Proposition 3.7.

Let K be a number field with $[K : \mathbb{Q}]$ with $K = \mathbb{Q}(\alpha)$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.[1] Let $m \in \mathbb{Z}[x]$ be the minimal polynomial for α. If p is prime and

$$m = q_1^{n_1} \cdots q_k^{n_k} \in \mathbb{Z}_p[x]\ ^{2}$$

for some distinct irreducible $q_1, \ldots, q_k \in \mathbb{Z}_p[x]$, then

(a) the prime ideals $P \subseteq \mathcal{O}_K$ such that $p \in P$ are exactly of the form $P = \langle q_i(\alpha), p \rangle$; and

(b) $\langle p \rangle = \langle q_1(\alpha), p \rangle^{n_1} \cdots \langle q_k(\alpha), p \rangle^{n_k}$ in $\mathcal{O}_K$.

[1] Observe that $K = \mathbb{Q}(\alpha)$ does not add any assumption, since every number field is of the form due to the primitive element theorem.

[2] To be more precise, we are referring to the polynomial $\overline{m} \in \mathbb{Z}_p[x]$ we obtain by replacing every coefficient of m by its equivalence class in $\mathbb{Z}_p$.

We shall treat this as a fact for now!

Example 3.4.

Consider $\alpha \in \mathbb{C}$ with $\alpha^2 + \alpha + 1 = 0$. Then $m = x^2 + x + 1$ is the minimal polynomial for α over $\mathbb{Q}$ and $\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]$.

Over $\mathbb{Z}_3$,

$$m = (x + 2)(x + 2),$$

so that

$$\langle 3 \rangle = \langle \alpha + 2, 3 \rangle^2.$$

On the other hand, over $\mathbb{Z}_2$, m is irreducible, so that

$$\langle 2 \rangle = \left\langle \alpha^2 + \alpha + 1, 2 \right\rangle.$$

Dedekind domains are the rings where the ideal prime factorization happens.

Recall.
Let R, S be integral domains, $R \subseteq S$.

(a) Let $\alpha \in S$. Then

$$\alpha \text{ is integral over } R \iff \text{there is monic } f \in R[x] \text{ such that } f(\alpha) = 0 \iff R[\alpha] \text{ is a finitely generated } R\text{-module.}$$

(b) We say S is integral over R if and only if every element of S is integral over R.

Def'n 3.2. **Integral Closure**
Let R, S be integral domains, $R \subseteq S$.

(a) The ***integral closure*** of R in S is
$$\{\alpha \in S : \alpha \text{ integral over } R\}.$$

(b) R is ***integrally closed*** if and only if the integral closure of R in its field of fractions is R.

Example 3.5.
$\mathbb{Z}$ is integrally closed.

Let K be a number field and let $R = \mathcal{O}_K$. Let F be the field of fractions of R. Given $\alpha \in K$, since α is an algebraic number, there is a polynomial $f \in \mathbb{Z}[x]$ annihilating α. Taking the leading coefficient $N \in \mathbb{Z}$ of f, it follows $N\alpha \in R$. Hence $\alpha \in F$, which imply that $K \subseteq F$.

But F is the smallest field containing R, so that $K = F$.

Proposition 3.8.
Let K be a number field. Then $\mathcal{O}_K$ is algebraically closed.

Proof. Let
$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathcal{O}_K[x]$$
and supose $f(\alpha) = 0$ for some $\alpha \in K$. Then each a_i is an algebraic integer, so $\mathbb{Z}[a_i]$ is a finitely generated $\mathbb{Z}$-module. Hence $\mathbb{Z}[a_{n-1}, \ldots, a_0]$ is also finitely generated. Also,
$$\alpha^n = -\sum_{j=0}^{n-1} a_j\alpha^j.$$
It follows that $\mathbb{Z}[\alpha, a_{n-1}, \ldots, a_0]$ is finitely generated. Since $\mathbb{Z}$ is Noetherian and $\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha, a_{n-1}, \ldots, a_0]$, $\mathbb{Z}[\alpha]$ is finitely generated. Thus α is an algebraic integer, as required.

QED

Def'n 3.3. **Dedekind Domain**
Let R be an integral domain. We say R is a ***Dedekind domain*** if

(a) R is Noetherian;

(b) R is integrally closed; and

(c) every nonzero prime ideal of R is maximal.

Example 3.6.
Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.

Here is a question for the section:

why is Def'n 3.3 the right definition for prime factorization?

It turns out (*spoiler alert*)...

(a) $\implies$ existence of prime factorization;

(b) $\implies$ prime ideals cannot be factored further; and

(c) $\implies$ uniqueness of prime factorization.

Let us first explore the third implication. The following lemma will be *the contradiction getter*, according to Blake.

Lemma 3.9.
Let R be a Dedekind domain and let I be a proper nontrivial ideal of R. Let F be the field of fractions of R. Then there is $\lambda \in F \setminus R$ such that $\lambda I \subseteq R$.

Proof. Let $a \in I$ be nonzero. Since R is Noetherian, we may find nonzero prime ideals $P_1, \ldots, P_r$ such that $P_1 \cdots P_r \subseteq \langle a \rangle$ by Proposition 3.2. Moreover, assume r is minimal (i.e. there does not exist fewer prime ideals $Q_1, \ldots, Q_k$ such that $Q_1 \cdots Q_k \subseteq \langle a \rangle$). Let M be a maximal ideal containing I.

Since $P_1 \cdots P_r \subseteq \langle a \rangle \subseteq I \subseteq M$ and M is prime, some P_i is contained in M. Without loss of generality, suppose $P_1 \subseteq M$. Since P_1 is a nonzero prime ideal of a Dedekind domain, it is maximal. Hence $P_1 = M$.

Case 1. $r = 1$.

In this case,

$$P_1 \subseteq \langle a \rangle \subseteq I \subseteq M = P_1,$$

so that $I = P_1$ is a prime ideal. Take $\lambda = a^{-1}$, so that

$$\lambda \langle a \rangle = a^{-1} \langle a \rangle = R \subseteq R.$$

A quick note: $a^{-1} \notin R$, since if $a^{-1} \in R$, then a is a unit in R, so that the principal ideal $\langle a \rangle$ *blows up to* R, contradicting the fact that $\langle a \rangle \subseteq I \neq R$.

(End of Case 1)

Case 2. $r > 1$.

By minimality of r, $P_2 \cdots P_r \nsubseteq \langle a \rangle$, so choose

$$b \in P_2 \cdots P_r \setminus \langle a \rangle .$$

Note that $bP_1 \subseteq \langle a \rangle$, since, given any $c \in P_1$, $bc \in (P_2 \cdots P_r) P_1 = P_1 \cdots P_r \subseteq \langle a \rangle$. Then

$$bI \subseteq bM = bP_1 \subseteq \langle a \rangle . \qquad [3.2]$$

Since $b \notin \langle a \rangle$, $\lambda = \frac{b}{a} \notin R$. By [3.2], given any $x \in I$, $bx = ar$ for some $r \in R$, so that

$$\lambda x = \frac{b}{a} x = \frac{ar}{a} = r \in R.$$

(End of Case 2)

QED

Proposition 3.10. Invertibility of the Ideals of a Dedekind Domain
Let R be a Dedekind domain and let I be an ideal of R. Then there exists a nonzero ideal $J \subseteq R$ such that IJ is principal.

Proof. The case where $I = \{0\}$ or $I = R$ is trivial. Hence suppose I is a nontrivial proper ideal.

Let $a \in I$ be nonzero. Consider

$$J = \{x \in R : xI \subseteq \langle a \rangle\} ,$$

which is a nonzero ideal of R (check this!). Note $IJ \subseteq \langle a \rangle$ by definition.

Let

$$A = \frac{1}{a} IJ.$$

Since $IJ \subseteq \langle a \rangle$, it follows $A \subseteq R$.

Suppose for contradiction $A \neq R$. Observe that A is a nonzero ideal of R (again, check this!). From Lemma 3.9, *the contradiction getter*, there is $\lambda \in F \setminus R$ such that $\lambda A \subseteq R$. Here F is the field of fractions of R. We note two things.

(a) *Stupidly*, $J = \frac{1}{a} aJ$. Since $a \in I$ and $A = \frac{1}{a} IJ$, this means $J \subseteq A$, so that

$$\lambda J \subseteq \lambda A \subseteq R.$$

(b) Observe that $\lambda A = \frac{\lambda}{a} IJ \subseteq R$. This means $\lambda IJ \subseteq aR = \langle a \rangle$.

But by the definition of J,

$$J = \{x \in R : xI \subseteq \langle a \rangle\},$$

it follows $\lambda J \subseteq J$. Say J is generated by $\alpha_1, \ldots, \alpha_m$. Then we may find $B \in R^{m \times m}$ such that

$$\begin{bmatrix} \lambda\alpha_1 \\ \vdots \\ \lambda\alpha_m \end{bmatrix} = B \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

That is, every $\lambda\alpha_j$ can be written as a R-linear combination of $\alpha_1, \ldots, \alpha_m$. This means

$$(\lambda I - B) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{bmatrix} = 0,$$

where at least one of α_j is nonzero as $J = \langle \alpha_1, \ldots, \alpha_m \rangle$. Hence

$$\det(\lambda I - B) = 0.$$

This means λ is a root of a monic polynomial over R, which contradicts the fact that R is integrally closed and $\lambda \notin R$.

Thus $A = R$, so that

$$IJ = aR = \langle a \rangle,$$

as required.

QED

Corollary 3.10.1.

Let R be a Dedekind domain and let

$$X = \{I \subseteq R : I \text{ is a nonzero ideal of } R\}.$$

Define an equivalence relation $\sim$ on X by

$$I \sim J \iff \exists \alpha, \beta \in R \setminus \{0\} \, [\alpha I = \beta J].$$

Then

$$\mathcal{G} = \{[I]_\sim : I \in X\}$$

is a group with multiplication

$$[I]\,[J] = [IJ].$$

Proof. This follows from Proposition 3.10 and Assignment 2.

QED

Def'n 3.4. **Ideal Class Group** of a Dedekind Domain

Consider the setting of Corollary 3.10.1. We call $\mathcal{G}$ the ***ideal class group*** of R.

Proposition 3.11. Cancellation of Ideals of Dedekind Domains

Let R be a Dedekind domain and let $A, B, C \subseteq R$ be nontrivial ideals. Then

$$AB = AC \implies B = C.$$

Proof. Let J be a nontrivial ideal of R such that

$$JA = \langle a \rangle$$

for some nonzero $a \in A$. Then

$$AB = AC \implies JAB = JAC \implies \langle a \rangle B = \langle a \rangle C \implies aB = aC \implies B = C,$$

where the last implication uses the fact that R is an integral domain.

QED

Def'n 3.5. **Ideal Divisibility**

Let R be a ring and let AB be ideals of R. We say A ***divides*** B, denoted as $A|B$, if and only if there is an ideal C of R such that $B = AC$.

Proposition 3.12. Characterization of Ideal Divisibility for Dedekind Domains

Let R be a Dedekind domain and let A, B be ideals of R. Then

$$A|B \iff B \subseteq A.$$

Proof. The case involving $\{0\}$ or R is trivial. Hence assume $A, B \neq \{0\}, R$.

($\implies$) Clearly $B = AC \subseteq A$.

($\impliedby$) Suppose $B \subseteq A$. Let J be a nonzero ideal such that $JA = \langle a \rangle$ for some $a \in A$. Then $JB \subseteq \langle a \rangle$, which means

$$C = \frac{1}{a} JB$$

is an ideal of R (again, we can *multiply* by $\frac{1}{a}$ since $JB \subseteq \langle a \rangle$). This means

$$JAC = \langle a \rangle \frac{1}{a} JB = JB.$$

Using cancellation (Proposition 3.11), we obtain

$$AC = B.$$

That is, $A|B$, as required.

QED

Proposition 3.12 is *nice*, since checking containment is easier than checking divisibility.

Theorem 3.13. Prime Factorization of Ideals of a Dedekind Domain

Let R be a Dedekind domain and let I be a proper nontrivial[1] ideal of R. Then I can be uniquely[2] written as a product of prime ideals.

[1]"*With R we can never get existence and with* $\{0\}$ *we can never get uniqueness, so we rule those cases out.*" - Blake

[2]Unique up to reordering.

Proof of Existence. Let X be the set of proper nontrivial ideals of R which cannot be written as a product of prime ideals. For contradiction, $X \neq \emptyset$. Let $I \in X$ be an maximal element of X. We know I is not prime, so is not maximal, since R is a Dedekind domain. Let P be a maximal ideal containing I. Since P is prime, $I \neq P$. Hence there is a proper ideal J such that $I = PJ$. Then

$$I = PJ \subseteq J.$$

If $I = J$, then observe that

$$RJ = RI = I = PJ,$$

so by cancelling J, we obtain $R = P$, which is a contradiction. Hence $I \neq J$, so that $J \notin X$. This means J is a product of prime ideals, so that $I = PJ$ is also a product of prime ideals, which is a contradiction.

Thus we conclude $X = \emptyset$, which means every proper nontrivial ideal of R can be written as a product of prime ideals.

Proof of Uniqueness. Suppose we have two factorizations of a proper nontrivial ideal I,

$$I = P_1 \cdots P_n = Q_1 \cdots Q_m,$$

where $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ are prime. This means

$$Q_1 \cdots Q_m \subseteq P_1.$$

Since P_1 is prime, it follows one of Q_j's is contained in P_1. Without loss of generality, assume $Q_1 \subseteq P_1$. But Q_1 is also prime and R is a Dedekind domain, so that Q_1 is maximal. This means $P_1 = Q_1$. So by cancellation,

$$P_2 \cdots P_n = Q_2 \cdots Q_m.$$

By induction, we obtain uniqueness.

QED

Now that we know prime factorization exists and is unique, our next question is

how do we actually factor an ideal?

This question will be answered in the following two sections.

4. Ideal Norm

Def'n 3.6. **Norm** of an Ideal

Let K be a number ring and let $R = \mathcal{O}_K$. If I is a nontrivial ideal of R, then we define the ***norm*** of I as

$$N(I) = |R/I|.$$

Let's see where definition can be handy. *Assume* that the norm is multiplicative:

$$N(IJ) = N(I)\,N(J).$$

Let I be a nontrivial proper ideal of R and let

$$n = N(I) = |R/I|.$$

We know that I can be factored into product of prime ideals

$$I = P_1^{n_1} \cdots P_k^{n_k}.$$

This means

$$N(I) = N(P_1)^{n_1} \cdots N(P_k)^{n_k}. \qquad [3.3]$$

Recall that

$$N(P_i) = |R/P_i| = p_i^{m_i}$$

where $p_i \in P_i$ is prime and $m_i \in \mathbb{N}$. Consequently,

$$n = p_1^{n_1 m_1} \cdots p_k^{n_k m_k},$$

implying that

$$p \in \mathbb{N} \text{ is prime with } p|n \implies p = p_i \text{ for some } i.$$

But

$$p = p_i \in P_i \implies \langle p \rangle \subseteq P_i \implies P_i | \langle p \rangle .$$

Hence *if* we can factor each $\langle p_i \rangle$, then we can find the candidates for P_i's and hence factor I. Also, due to [3.3], $N(I)$ helps us find n_i as well.

Therefore, here are the goals in order for the above story to work out.

Goals

(a) Prove that ideal norm is multiplicative.

(b) Show $\langle p \rangle$ is easily factored for *almost all*[1] prime $p \in \mathbb{N}$.

[1] What does *almost all* mean? We shall see this later.

Suppose

$$I = P_1^{n_1} \cdots P_k^{n_k} \subseteq \mathcal{O}_K$$

with $P_i \neq P_j$ for $i \neq j$. Since P_i's are coprime, it follows that

$$R/I \cong R/P_1^{n_1} \times \cdots \times R/P_k^{n_k}$$

by the Chinese remainder theorem. Hence

$$N(I) = N(P_1^{n_1}) \cdots N\left(P_k^{n_k}\right).$$

Hence it suffices to show that

$$N(P^n) = N(P)^n \text{ for } n \in \mathbb{N}, \text{ prime } P. \tag{3.4}$$

Here are the tools to prove [3.4]:

(a) localization;

(b) local rings; and

(c) discrete valuation ring.

Suppose $R = \mathcal{O}_K$ with an integral basis $\{v_1, \ldots, v_n\}$, and let I be a nonzero ideal of R. Then by Assignment 2,

$$\operatorname{disc}(w_1, \ldots, w_n) = [R : I]^2 \operatorname{disc}(v_1, \ldots, v_n) = N(I)^2 \operatorname{disc}(K).$$

In the special case I is principal,

$$I = \langle \alpha \rangle$$

for some $\alpha \neq 0$, $\{\alpha v_1, \ldots, \alpha v_n\}$ is an integral basis for I. Then

$$\operatorname{disc}(\alpha v_1, \ldots, \alpha v_n) = N(I)^2 \operatorname{disc}(K). \tag{3.5}$$

On the other hand,

$$\operatorname{disc}(\alpha v_1, \ldots, \alpha v_n) = \det\left(\left[\sigma_i(\alpha v_j)\right]_{i,j=1}^n\right)^2 = \left(\prod_{j=1}^n \sigma_j(\alpha)\right)^2 \det\left(\left[\sigma_i(v_j)\right]_{i,j=1}^n\right)^2 = N_{K/\mathbb{Q}}(\alpha)^2 \operatorname{disc}(K). \tag{3.6}$$

It follows from [3.5], [3.6] that

$$N(I)^2 = N_{K/\mathbb{Q}}(\alpha)^2 \implies N(\langle \alpha \rangle) = \left|N_{K/\mathbb{Q}}(\alpha)\right|.$$

Recall that the goal is to prove multiplicativity of ideal norm by showing

$$N(P^n) = N(P)^n$$

for a prime ideal P.

Def'n 3.7. **Local Ring**
A ***local ring*** is a ring R which has a unique maximal ideal.

How do we spot a local ring? Here is Blake's favorite way.

Proposition 3.14.
Let R be a ring. Then

$$R \text{ is local} \iff R \setminus R^\times \text{ is an ideal of } R.$$

In this case, $R \setminus R^\times$ is the unique maximal ideal of R.

Proof. Let $I = R \setminus R^\times$.
($\implies$) Suppose R is local with a unique maximal ideal M. Since M is proper, M does not have any units, so that

$$M \subseteq I.$$

But $I \subseteq \langle I \rangle \subseteq M$, since I does not have any units and M is the unique maximal ideal.
($\impliedby$) Suppose I is an ideal. Then for any maximal ideal $M \subseteq R$, $M \subseteq I$, since M does not have any unit. But M is maximal, so $M = I$.

QED

Example 3.7.
Fields are local.

Example 3.8.
Consider $\mathbb{Z}_{p^n}$ with $n > 1$. Then

$$x \notin \mathbb{Z}_{p^n}^\times \iff \gcd(x, p^n) \neq 1 \iff p | x \iff x \in \langle p \rangle,$$

so $\langle p \rangle$ is the unique maximal ideal for $\mathbb{Z}_{p^n}$. Thus $\mathbb{Z}_{p^n}$ is local.

How can we construct local integral domains? The answer is *localization*.

"Localization is a process of making a local ring." - Blake

There are three ingredients to localization: an integral domain, the field of fractions and a prime ideal.

Def'n 3.8. **Localization**
Let R be an integral domain, let K be the field of fractions and let P be a prime ideal. The ***localization*** of R at P is

$$R_P = \left\{ \frac{a}{b} \in K : b \notin P \right\}.$$

There's more general version of localization, but let's leave that to commutative algebraists.

Observe that we are using a *lazy notation*. In fact, we can have $\frac{a}{b} \in R_P$ when $b \in P$. What we need is for there to exist $c, d \in R$ such that $\frac{a}{b} = \frac{c}{d}$ but $d \notin P$. The following example demonstrates this remark.

Example 3.9.
Consider $R = \mathbb{Z}, P = \langle 2 \rangle$. Then $\frac{4}{6}$ *looks like* it should not belong to $\mathbb{Z}_{\langle 2 \rangle}$, since $2|6$. However, $\frac{4}{6} = \frac{2}{3}$ and $2 \nmid 3$, so that $\frac{4}{6} \in \mathbb{Z}_{\langle 2 \rangle}$.

Let $\frac{a}{b}, \frac{c}{d} \in K$ with $b, d \notin P$. Then
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in R_P,$$
since $bd \notin P$.[3] In a similar manner
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in R_P.$$
Hence R_P is a subring of K.

Observe that
$$R_P \setminus R_P^\times = PR_P = \left\{ \sum_{j=1}^{n} a_j r_j : a_j \in P, r_j \in R_P \right\}. \tag{3.7}$$
Proving [3.7] is left as an exercise.

In particular, $R_P \setminus R_P^\times$ is an ideal, so by Proposition 3.14 R_P is local.

Since we are going to refer PR_P often, let's give it a notation.

Notation 3.9. P_P
We write P_P to denote PR_P.

It turns out
$$P_P = \left\{ \frac{a}{b} : a \in P, b \notin P \right\},$$
which is also left as an exercise.

We know that
$$R \text{ is an integral domain} \implies R_P \text{ is local.}$$
Well, Dedekind domains are *much better* than integral domain, so it must be the case that
$$R \text{ is a Dedekind domain} \implies R_P \text{ is local} + ???.$$

6. Discrete Valuation Rings (DVRs)

Def'n 3.10. **Discrete Valuation Ring (DVR)**
A ***DVR*** is an integral doamin which is

(a) not a field;
(b) Noetherian;
(c) local; and
(d) such that the unique maximal ideal is principal.

A generator π for the unique maximal ideal is called a ***uniformizer***.

Here's another goal:
$$R \text{ is Dedekind and } P \text{ is a nontrivial proper ideal of } R \implies R_P \text{ is a DVR.} \tag{3.8}$$
And indeed, [3.8] is why DVR's are created.

We are ruling out the case $P = \{0\}$, since $P = \{0\}$ implies R_P is the field of fractions of R, so not a DVR.

[3] *"The complement of a prime ideal is multiplicatively closed."* - Blake

Lemma 3.15. Nakayama

Let R be a ring and let I be a nonzero proper ideal of R. Let M be a finitely generated R-module with $IM = M$. Then there exists $a \in R$ such that

(a) $a + I = 1 + I$; and

(b) $aM = 0$.

Proof. Since M is finitely generated,

$$M = Rx_1 + \cdots + Rx_n$$

for some $x_1, \ldots, x_n \in M$. But $IM = M$, so that we may write

$$x_i = a_{i,1}x_1 + \cdots + a_{i,n}x_n$$

for some $a_{i,1}, \ldots, a_{i,n} \in I$. Consider the matrix

$$A = \left[a_{i,j}\right]_{i,j=1}^{n} \in I^{n\times n}.$$

Let

$$v = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Then by construction

$$Av = v.$$

Also, consider

$$f = \det\left(xI_n - A\right).$$

Then by the Cayley-Hamilton theorem, we have

$$f(A) = 0.$$

Writing f explicitly,

$$f = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0,$$

where each $c_i \in I$. Hence

$$0 = f(A)\,v = \left(A^n + c_{n-1}A^{n-1} \cdots + c_1A + c_0I_n\right)v = v + c_{n-1}v + \cdots c_1v + c_0v = f(1)\,v.$$

So let $a = f(1)$.

Now,

$$av = 0 \implies ax_i = 0 \implies aM = a\left(Rx_1 + \cdots + R_n\right) = 0.$$

Also,

$$a = f(1) = 1 + c_{n-1} + \cdots + c_1 + c_0 \equiv 1 \bmod I,$$

since each $c_i \in I$.

QED

Proposition 3.16.

Let R be a DVR and $M = \langle \pi \rangle$ be the unique maximal ideal of R. Then every nonzero proper ideal I of R is of the form

$$I = M^n$$

for some $n \in \mathbb{N}$.

Proof. Let I be a nonzero proper ideal and let $J = \frac{1}{\pi}R$. Then

$$JM = R.$$

Then

$$I = IR = \underbrace{IJ}_{=I_1}M.$$

But $I \subseteq M = \langle \pi \rangle$, so that $I_1 \subseteq R$. Hence

$$I = I_1 M \subseteq I_1.$$

Suppose $I = I_1$. Then $I = IM$. Also I is finitely generated, since R is a DVR so is Noetherian. Hence by Nakayama's lemma (with the roles of I, M switched) there is $a \in R$ such that $a - 1 \in M$ and $aI = 0$. Since R is an integral domain,

$$a = 0 \implies -1 \in M \implies M = R.$$

This is a contradiction. Hence I is a proper subset of I_1.

If $I_1 = R$, then $I = M$, and we are done. Suppose $I_1 \neq R$. Then

$$I_1 = I_1 R = \underbrace{I_1 J}_{=I_2} M \subseteq I_2.$$

Similarly, we have that $I_1 \neq I_2$ due to Nakayama's lemma.

If $I_2 = R$, then

$$I_1 = M \implies I = I_1 M = M^2$$

and we are done. If not, we continue the process to obtain an ascending chain of ideals $(I_n)_{n=1}^{\infty}$. Since R is Noetherian, this chain stabilizes, so that we have $n \in \mathbb{N}$ such that $I_n = M$. This means I is a power of M, as required.

QED

Observe that, by Proposition 3.16, every ideal of a DVR is principal. As a consequence, we are going to prove

$$\text{DVR} \iff \text{local PID not a field.}$$

Let R be a DVR and let $M = \langle \pi \rangle$ be the unique maximal ideal of R. Let $x \in R$ be nonzero. We can classify x into two cases.

(a) $x \in R^\times$.

(b) $x \notin R^\times$, so that $\langle x \rangle$ is a proper nonzero ideal. So by Proposition 3.16, $\langle x \rangle = \langle \pi^n \rangle$. This means x, π are *associates*: $x = u\pi^n$ for some unit $u \in R^\times$. This makes every element of R look *quite uniform*, which is why we call π a *uniformizer*.

Proposition 3.17.

Let R be a Noetherian integral domain and let P be a nonzero prime ideal of R. Then R_P is Noetherian.

Proof. Let $I \subseteq R_P$ be an ideal and let $J = I \cap R$ be an ideal of R. Then J is a finitely generated R-module, so that

$$J = Rx_1 + \cdots + Rx_n$$

for some $x_1, \ldots, x_n \in R$. Let $x \in I$ with $x = \frac{a}{b}$ for some $a, b \in R$ with $b \notin P$. This means

$$a = bx \in I \cap R = J.$$

Thus

$$a = r_1 x_1 + \cdots + r_n x_n \implies x = \frac{a}{b} = \frac{r_1}{b} x_1 + \cdots + \frac{r_n}{b} x_n \implies I = R_P x_1 + \cdots + R_P x_n.$$

QED

Theorem 3.18.

Let R be a Dedekind domain and let P be a nonzero prime ideal. Then R_P is a DVR.

Proof. Since P is a nonzero ideal, we know R_P is not a field. Also, since R is a Dedekind domain, R is Noetherian, so R_P is Noetherian. Moreover, R_P is local as a localization of a ring. Hence it remains to show that the unique maximal ideal of R_P, namely P_P (i.e. the ideal of non-units of R_P) is principal.

Recall that there exists an ideal I such that

$$IP = \langle \alpha \rangle$$

for some $\alpha \in P$. Consider $J = \frac{1}{\alpha} I$. Note

$$JP = \frac{1}{\alpha} IP = \frac{1}{\alpha} \langle \alpha \rangle = R.$$

Say

$$1 = a_1 b_1 + \cdots + a_n b_n,$$

where each $a_i \in J, b_i \in P$. Take i such that $a_i b_i \notin P$ (such i exists, since otherwise $1 \in P$ where P is a prime ideal). This means

$$\frac{1}{a_i b_i} \in R_P.$$

Let $x \in P_P$. Then $y = \frac{x}{a_i b_i} \in P_P$, since $x \in P_P$. Moreover

$$x = a_i b_i y.$$

Say

$$y = \frac{u}{v}$$

for some $u \in P, v \in R \setminus P$. Then

$$x = b_i \frac{a_i u}{v}.$$

But $a_i \in J, u \in P$ so that $a_i u \in JP = R$. Hence $\frac{a_i u}{v} \in R_P$, which means

$$x \in \left\langle \frac{b_i}{1} \right\rangle \subseteq R_P.$$

Since x was arbitrary, it follows

$$P_P = \left\langle \frac{b_i}{1} \right\rangle,$$

as required.

QED

Theorem 3.18 does two awesome things for us.

(a) It proves the multiplicativitiy of ideal norm.

(b) It gives a powerful way to prove whether a ring of integers is of the form $\mathbb{Z}[\alpha]$.

7. Multiplicativity of the Ideal Norm

Proposition 3.19.
Let R be an integral domain and let P be a nonzero prime ideal. Then for all $n \in \mathbb{N}$,

$$R/P^n \cong R_P/P_P^n.$$

Proof Sketch. The isomorphism is given by

$$r + P^n \mapsto \frac{r}{1} + P_P^n.$$

QED

Recall.
Let R be an integral domain and suppose an ideal $I \subseteq R$ is such that

$$I = P_1^{n_1} \cdots P_k^{n_k}$$

for some pairwise coprime prime ideals $P_1, \ldots, P_k$ of R. Then by the CRT,

$$R/I \cong R/P_1^{n_1} \times \cdots \times R/P_k^{n_k}.$$

If $R = \mathcal{O}_K$ for some number field K, then

$$N(I) = N(P_1^{n_1}) \cdots N\left(P_k^{n_k}\right).$$

Hence it suffices to show

$$N(P^n) = N(P)^n$$

for any prime ideal $P \subseteq R$ and $n \in \mathbb{N}$.

Proposition 3.20.
Let R be a DVR and let P be a maximal ideal of R. If R/P is finite, then

$$|R/P^n| = |R/P|^n$$

for all $n \in \mathbb{N}$.

Proof. We use induction on n.

Suppose

$$\left|R/P^{n-1}\right| = |R/P|^{n-1}$$

for some $n > 1$. Consider

$$\begin{aligned} \varphi : R/P^n &\to R/P^{n-1} \\ r + P^n &\mapsto r + P^{n-1} \end{aligned}.$$

Since $P^n \subseteq P^{n-1}$, φ is well-defined. Clearly φ is an epimorphism. Moreover,

$$\ker(\varphi) = P^{n-1}/P^n$$

By the first isomorphism theorem on φ (or the third isomorphism theorem alternatively),

$$(R/P^n) \,/\, \left(P^{n-1}/P^n\right) \cong R/P^n.$$

This implies

$$|R/P^n| = \left|P^{n-1}/P^n\right| |R/P|^n.$$

Hence it remains to show $\left|P^{n-1}/P^n\right| = |R/P|$.

Since P is a maximal ideal, $F = R/P$ is a field. Consider $V = P^{n-1}/P^n$ as a F-vector space with the scalar multiplication

$$(r + P)(a + P^n) = ra + P^n.$$

Say $P = \langle \pi \rangle$. Let $x \in V$. Then

$$x = a + P^n$$

for some $a \in P^{n-1}$. That is, $a \in \left\langle \pi^{n-1} \right\rangle$, so that $a = c\pi^{n-1}$ for some $c \in R$. Hence

$$x = a + P^n = c\pi^{n-1} + P^n = (c + P)\left(\pi^{n-1} + P^n\right).$$

Since x was arbitrary, it follows $\pi^{n-1} + P^n$ spans V, so that $\dim_F(V) = 1$. That is, $V \cong F$ as F-vector spaces. Thus

$$\left|P^{n-1}/P^n\right| = |V| = |F| = |R/P|.$$

QED

Theorem 3.21. Multiplicativity of the Ideal Norm

Let $R = \mathcal{O}_K$ for some number field K. If I, J are nonzero ideals of R, then

$$N(IJ) = N(I)\,N(J)\,.$$

Proof. Let P be a nonzero prime ideal of R. It suffices to show

$$N(P^n) = N(P)^n\,.$$

But:

$$N(P^n) = |R/P^n| = |R_P/P_P^n| = |R_P/P_P|^n = |R/P|^n = N(P)^n\,.$$

QED

8. Further Application of DVR's

Theorem 3.22. DVR Characterization

Let $R = \mathcal{O}_K$ and let $S \subseteq R$ be a subring such that $[R:S] = n < \infty$ (index as an additive subgroup).

(a) $S = R$ if and only if S_P is a DVR for all nonzero prime ideal $P \subseteq S$.

(b) Let $P \subseteq S$ be a prime ideal and let $p \in P$ be a prime number.[1] If $p \nmid n$, then S_P is a DVR.

[1] Again, such a prime exists due to Lagrange.

(a) itself alone is not practical, since it is difficult to prove S_P is a DVR for all prime $P \subseteq S$. (b) simplifies things a lot.

Note that (b) is a *huge* generalization of

$$\text{squarefree disc}(\alpha) \implies \mathcal{O}_{\mathbb{Q}(\alpha)} = \mathbb{Z}[\alpha]\,.$$

Here is an explanation.

Consider the case

$$K = \mathbb{Q}(\alpha)\,, \alpha \in \mathcal{O}_K = R, S = \mathbb{Z}[\alpha]\,, \operatorname{rank}(R) = \operatorname{rank}(S) = [K:\mathbb{Q}]\,. \tag{3.9}$$

By Assignment 2, we know

$$[R:S] < \infty.$$

Moreover,

$$\operatorname{disc}(\alpha) = [R:S]^2 \operatorname{disc}(K)\,.$$

Therefore,

$$p^2 \nmid \operatorname{disc}(\alpha) \implies p \nmid [R:S]\,.$$

Hence, when $\operatorname{disc}(\alpha)$ is squarefree in particular, the above implication always holds, so by Theorem 3.22 S_P is a DVR for any prime $P \subseteq S$.

But *sometimes* (and by sometimes we mean *always*) we have $p \in P$ such that $p|n$. What should we do in that case?

Proposition 3.23.

Let $\alpha \in \mathbb{A}$, let $f \in \mathbb{Z}[x]$ be the minimal polynomial for α, and let $p \in \mathbb{Z}$ be prime. Say

$$f = p_1^{n_1} \cdots p_k^{n_k}$$

is the irreducible factorization of f in $\mathbb{Z}_p[x]$. Then the prime ideals of $\mathbb{Z}[\alpha]$ which has p are exactly $\langle p_i(\alpha)\,, p\rangle$.

Assignment 6

Proposition 3.23 does not say

$$\langle p \rangle = \langle p_1(\alpha), p \rangle^{n_1} \cdots \langle p_k(\alpha), p \rangle^{n_k}.$$

A counterexample is when $\alpha = \sqrt{5}$.

Again, consider the case in [3.9]. Let $P \subseteq S$ be a nonzero prime ideal. Then

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x] / \langle f \rangle,$$

where f is the minimal polynomial for α. Now, $\mathbb{Z}[x]$ is Noetherian due to *Hilbert's basis theorem*,[4] and quotients of a Noetherian ring is Noetherian. Hence $\mathbb{Z}[\alpha]$ is Noetherian, so that S_P is local, Noetherian, and not a field.

Hence in practice, we need only check that P_P is principal.

Example 3.10.

Let $f = x^4 - 5x^2 + 7$, which is irreducible over $\mathbb{Q}$. Then $\operatorname{disc}(f) = 1008 = 2^4 3^2 7^1$. Let $\alpha \in \mathbb{C}$ be a root of f and let $K = \mathbb{Q}(\alpha)$. Let $R = \mathcal{O}_K$ and let $S = \mathbb{Z}[\alpha]$. Prove $S = R$.

Proof. It suffices to show that every prime ideal which has 2 or 3 is a DVR.

Case 1. $p = 2$.

Observe

$$f = x^4 + x^2 + 1 = \left(x^2 + x + 1\right)^2$$

over $\mathbb{Z}_2$. Hence the only prime ideal of S which has 2 is $P = \left\langle \alpha^2 + \alpha + 1, 2 \right\rangle$. By the above comment, it suffices to check P_P is a principal ideal of S_P.

Dividing f by $x^2 + x + 1$ over $\mathbb{Z}$, we obtain

$$f = \left(x^2 - x - 5\right)\left(x^2 + x + 1\right) + (6x + 12).$$

This means

$$0 = f(\alpha) = \left(\alpha^2 + \alpha + 1\right)\left(\alpha^2 - \alpha - 5\right) + (6\alpha + 12) \implies 6\alpha + 12 \in P.^1$$

Dividing by 2,

$$2(3\alpha + 6) \in \left(\alpha^2 + \alpha + 1\right) S.$$

Suppose for contradiction $3\alpha + 6 \in P$. Then

$$3\alpha + 6 \in P \implies 3\alpha \in P \implies \alpha \in P \implies 1 \in P,$$

since α divides $\alpha^2 + \alpha$. Since P is prime, this is a contradiction.

Hence

$$-2(3\alpha + 6) = \left(\alpha^2 + \alpha + 1\right)\left(\alpha^2 - \alpha - 5\right) \implies 2 = \frac{-1}{3\alpha + 6}\left(\alpha^2 + \alpha + 1\right)\left(\alpha^2 - \alpha - 5\right)$$

in S_P, so that

$$2 \in \left(\alpha^2 + \alpha + 1\right) S_P \implies P_P = 2S_P + \left(\alpha^2 + \alpha + 1\right) S_P = \left(\alpha^2 + \alpha + 1\right) S_P.$$

Thus S_P is principal.

(End of Case 1)

Case 2. $p = 3$.

Observe

$$f = x^4 + x^2 + 1 = (x + 1)^2 (x + 2)^2$$

[4] Another stolen fact from commutative algebra!

over $\mathbb{Z}_3$. Hence the prime ideals of S which has 3 are $\langle \alpha+1, 3\rangle, \langle \alpha+2, 3\rangle$. Over $\mathbb{Z}$, we have

$$f(-2) = f(-1) = 3.$$

Using the remainder theorem, this means

$$f = (x+1)\,q_1 + f(-1) = (x+1)\,q_1 + 3 \implies 0 = f(\alpha) = (\alpha+1)\,q_1(\alpha) + 3 \implies 3 \in \langle \alpha+1\rangle.$$

Similarly $x \in \langle \alpha+2\rangle$. Hence $P_1 = (\alpha+1)\,S, P_2 = (\alpha+2)\,S$. Thus

$$P_{1P_1} = (\alpha+1)\,S_{P_1},$$
$$P_{2P_2} = (\alpha+2)\,S_{P_2},$$

so that S_{P_1}, S_{P_2} are DVR's.

(End of Case 2)

---

[1] Of course, we can *easily* see $6\alpha + 12 \in P$ since 2 divides it. However, how are we supposed to know it is the *right* multiple of 2 to look at without this computation?

QED

To practive calculations, visit `lmfdb.org`.

Recall.
Let R be a DVR and let $M = \langle \pi \rangle$ be the unique maximal ideal of R. Let K be the field of fractions of R and let $x \in R$ be nonzero and nonunit. That is, $\langle x\rangle$ is a proper ideal of R. Then we know for some $m \in \mathbb{N}$

$$\langle x\rangle = \langle \pi\rangle^m = \langle \pi^m\rangle. \qquad [3.10]$$

In other words, [3.10] is the unique way of factoring any nonzero proper ideal of R.

Moreover, it follows from [3.10] that

$$x = u\pi^m$$

for some $u \in R^\times$. This is why we called π a *uniformizer*.

Therefore, for any $y \in K$, there are $m \in \mathbb{Z}, u \in R^\times$ such that

$$y = u\pi^m \implies y \in R \text{ or } \frac{1}{y} = u^{-1}\pi^{-m} \in R. \qquad [3.11]$$

Example 3.11.
Consider $f = x^3 + 2x - 8 \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$ with $\operatorname{disc}(f) = -1760 = -2^5 5^1 11^1$. Let $\alpha \in \mathbb{C}$ be a root of f, $K = \mathbb{Q}(\alpha), R = \mathcal{O}_K, S = \mathbb{Z}[\alpha]$. Then $R \neq S$.

Proof. Observe that

$$f = x^3$$

over $\mathbb{Z}_2$, so that $P = \langle \alpha, 2\rangle$ is the unique prime ideal of S which has 2.

To show $R \neq S$, it suffices to show that S_P is not a DVR. As always, proving this is equivalent to showing P_P is not principal. Suppose P_P is principal, say $P_P = \langle \pi\rangle$ for some $\pi \in S_P$, for contradiction. Then we have

$$\alpha = u_1\pi^n, 2 = u_2\pi^m$$

for some $u_1, u_2 \in R^\times$ and $n, m \in \mathbb{N}$. By [3.11], this means $\frac{\alpha}{2} \in S_P$ or $\frac{2}{\alpha} \in S_P$.

Case 1. *Suppose* $\frac{\alpha}{2} \in S_P$.

This means

$$\frac{\alpha}{2} = \frac{a + b\alpha + c\alpha^2}{d + e\alpha + k\alpha^2}$$

for some $a, b, c, d, e, k \in \mathbb{Z}$, where $d + e\alpha + k\alpha^2 \notin P$. So

$$d\alpha + e\alpha^2 + k(-2\alpha + 8) = 2a + 2b\alpha + 2c\alpha^2$$

using relation $f(\alpha) = 0$. Since $1, \alpha, \alpha^2$ form a basis, it follows

$$d - 2k = 2b$$

using the coefficients of α. This means

$$d = 2k + 2b \in P,$$

so that $d + e\alpha + k\alpha^2 \in P$, which is a contradiction.

(End of Case 1)

Case 2. *Suppose* $\frac{2}{\alpha \in S_P}$.

This means

$$\frac{2}{\alpha} = \frac{a + b\alpha + c\alpha^2}{d + e\alpha + k\alpha^2}$$

for some $a, b, c, d, e, k \in \mathbb{Z}$, where $d + e\alpha + k\alpha^2 \notin P$. So

$$2d + 2e\alpha + 2k\alpha^2 = a\alpha + b\alpha^2 + c(-2\alpha + 8) \implies 2d = 8c \implies d = 4c \in P \implies d + e\alpha + k\alpha^2 \in P,$$

which is a contraidction.

(End of Case 2)

QED

Example 3.12.

Consider $f = x^3 - x^2 + 5x + 1 \in \mathbb{Q}[x]$ which is irreducible over $\mathbb{Q}$ with $\mathrm{disc}(f) = -2^2 3^1 7^2$. Let $\alpha \in \mathbb{C}$ be a root of f, $K = \mathbb{Q}(\alpha)$, $R = \mathcal{O}_K$, $S = \mathbb{Z}[\alpha]$. Is $R = S$?

Answer. Observe

$$f = (x+1)^3$$

over $\mathbb{Z}_2$, so $P = \langle \alpha + 1, 2 \rangle$ is the unique maximal ideal of S which has 2.

Over $\mathbb{Z}$, we have

$$f(-1) = -6 \implies f = (x+1)q - 6$$

for some $q \in \mathbb{Z}[x]$, so that

$$0 = (\alpha + 1) q(\alpha) - 6 \implies 6 \in \langle \alpha + 1 \rangle .$$

Since $3 \notin P$,[5] we have

$$2 = \frac{1}{3} 6 \in (\alpha + 1) S_P \implies P_P = (\alpha + 1) S_P.$$

Moreover, over $\mathbb{Z}_7$,

$$f = (x+2)^3 ,$$

so that $Q = \langle \alpha + 2, 7 \rangle$ is the unique prime ideal of S which has 7. Over $\mathbb{Z}$,

$$f(-2) = -21 \implies 21 \in \langle \alpha + 2 \rangle \subseteq S \implies 7 = \frac{1}{3} 21 \in (\alpha + 2) S_Q \implies Q_Q = (\alpha + 2) S_Q.$$

Hence P_P is principal for any prime $P \subseteq S$, which means $R = S$.

QED

[5] $2 \in P$ implies $p \notin P$ for any prime $p \in \mathbb{N}$, since otherwise $1 \in P$ so P blows up to S.

We shall prove Theorem 3.22 now:

Theorem 3.22. DVR Characterization

Let $R = \mathcal{O}_K$ and let $S \subseteq R$ be a subring such that $[R : S] = n < \infty$ (index as an additive subgroup).

(a) $S = R$ if and only if S_P is a DVR for all nonzero prime ideal $P \subseteq S$.

(b) Let $P \subseteq S$ be a prime ideal and let $p \in P$ be a prime number.[1] If $p \nmid n$, then S_P is a DVR.

[1] Again, such a prime exists due to Lagrange.

Here is a little remark on the assumption $[R : S] = n < \infty$. Recall that

$$K = \operatorname{frac}(R).$$

For all $r \in R$, observe

$$nr + S = n(r + S) = 0 + S$$

in R/S, so that $nr \in S$. This means, given any $\frac{a}{b} \in K$,

$$\frac{a}{b} = \frac{na}{nb} \in \operatorname{frac}(S),$$

so that

$$\operatorname{frac}(R) = K = \operatorname{frac}(S).$$

It follows that, if $P \subseteq S$ is a prime ideal, then

$$\operatorname{frac}(S_P) = K.$$

Lemma 3.24. Lying-over Theorem

Let S, R be integral domains with $S \subseteq R$ and suppose R is integral over S. Let $P \subseteq S$ be a prime ideal. Then there is a prime ideal $Q \subseteq R$ such that $P = S \cap Q$.

Proof Sketch. Consider

$$R_P = \left\{ \frac{a}{b} : a \in R, b \in S \setminus P \right\}.$$

Claim 1. *R_P is a local ring.*

Exercise!

(End of Claim 1)

Clearly, $S_P \subseteq R_P$. Moreover, using the fintely generated module trick, we can show R_P is integral over S_P. Let $M \subseteq R_P$ be the unique maximal ideal of R_P and let $Q = M \cap R$. By Assignment 1, Q is prime. Moreover,

$$Q \cap S = (M \cap R) \cap S = (M \cap S_P) \cap S.$$

By Assignment 1, it follows $M \cap S_P$ is maximal. That is, $M \cap S_P = P_P$, since S_P is a local ring. Hence

$$Q \cap S = P_P \cap S = P,$$

as required.

QED

Proof of Theorem 3.22 (a)

It suffices to prove the reverse direction.

Suppose S_P is a DVR for all nonzero prime ideal $P \subseteq S$. Observe $R = \mathcal{O}_K$ is integral over S, as $S \supseteq \mathbb{Z}$ and R is integral over $\mathbb{Z}$. Let P be a nonzero prime ideal of S, so that there is prime $Q \subseteq R$ such that $P = Q \cap S$ by the lying-over theorem.

Claim 1. $S_P = R_Q$.

($\subseteq$) Let $x \in S_P$. This means

$$x = \frac{a}{b}$$

for some $a, b \in S$, $b \notin P$. That is, $a, b \in R$, $b \notin Q$ (as $P = Q \cap S$), so that

$$x \in R_Q.$$

($\supseteq$) Let $\alpha \in K \setminus S_P$. Then

$$\alpha = u\pi^n,$$

where π is a uniformizer for S_P, $u \in S_P^\times$ and $n \in \mathbb{Z}$. Since $\alpha \notin S_P$, it follows $n < 0$. This means $-1 - n \geq 0$, so that

$$\pi^{-1} = \underbrace{\pi^{-1-n}}_{\in S_P} \underbrace{\pi^n}_{\in S_P[\alpha]} \in S_P[\alpha] \implies S_P[\alpha] = K.$$

However, $S_P \subseteq R_Q \subset K$, where the last containment is proper since Q is nonzero. Thus $\alpha \notin R_Q$ (otherwise $R_Q \supseteq S_P[\alpha] = K$).

(End of Claim 1)

Let's *unfix* P, Q.

Let $y \in R$ and consider

$$D = \{b \in S : by \in S\}.$$

Immediately, D is an ideal of S.

Claim 2. $D = S$.

Suppose $D \neq S$ and let $P \subseteq S$ be a prime ideal containing D. Consider a prime ideal $Q \subseteq R$ with $P = S \cap Q$. From before,

$$S_P = R_Q.$$

If $y = \frac{a}{b}$ with $a, b \in S$, then

$$by = a \in S \implies b \in D \subseteq P.$$

Hence $y \notin S_P = R_Q$. But $y \in R \subseteq R_Q$, this is a contradiction. Hence $D = S$.

(End of Claim 2)

Using $1 \in D$,

$$y \in R \implies y \in S \implies S = R.$$

Proof of 3.22(b). Let $P \subseteq S$ be a prime ideal and let $p \in P$ be a prime number. Suppose $p \nmid n$. Since $p \in P$ and $\gcd(p, n) = 1$, $n \notin P$ by Lagrange's theorem. As before, consider

$$P = Q \cap S.$$

Since R_Q is a DVR, it suffices to prove the following claim.

Claim 1. $S_P = R_Q$.

We know $S_P \subseteq R_Q$.

(End of Claim 1)

QED