Notes on basics of algebraic NT

Daksh Aggarwal

December 24, 2020

1 Algebra

The purpose of this section is to explain the basic definitions and results of field theory and Galois theory that are important for algebraic number theory. The algebraic structures we will mainly encounter are groups and rings usually in the form of fields. We won't require much theory about groups and so we will concentrate on fields. Our rings will always have a multiplicative identity and almost always be commutative.

1.1 Field Extensions

Definition 1.1 (Field) A *field* is a commutative ring whose nonzero elements form a group under multiplication. In other words, we can divide by nonzero elements of the ring.

Recall that in $\mathbb{Z}$ we have a Fundamental Theorem of Arithmetic (FTA) that gurantees a unique factorization of any integer into primes. In algebraic number theory, we want to recover this theorem in more general rings. These rings will occur naturally as subrings of certain fields that contain the field of rationals $\mathbb{Q}$.

Definition 1.2 (Field extension) A field L is a *field extension* of a field K if $K \subseteq L$. More generally, L is a field extension of K if there is a ring homomorphism $K \to L$, called an embedding of K in L. This relationship is denoted L/K.

Notice that for a field extension L/K, we can view L as a vector space over K $-$ the axioms for a vector space are directly implied by the field axioms. So we then have a notion of a basis for L when viewed as a K-vector space and can therefore talk about a dimension of L.

Definition 1.3 (Degree) The *degree* of a field extension L/K is the dimension $\dim_K L$ of L as a K-vector space and is denoted $[L : K]$.

We will care only about finite field extensions L/K here, i.e., $[L : K] < \infty$. We now prove a basic fact worth remembering about degrees of field extensions, to illustrate the ideas introduced so far.

Lemma 1.4 *Let L, K, F be fields. If L is a finite extension of K and K is a finite extension of F, then L is a finite extension of F. Further, $[K : F] = [K : L][L : F]$.*

Proof. Let $n = [L : K]$ and $m = [K : F]$. Then there exists bases $\alpha_1, \alpha_2, \ldots, \alpha_n$ for L/K and $\beta_1, \beta_2, \ldots, \beta_m$ for K/F. The simplest idea works: we show the elements $\alpha_i\beta_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$, form a basis for L/F. Fix an element $k \in K$. Then we can write

$$k = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n, \tag{1.1}$$

with $a_i \in K$. Now, each $a_i \in K$ can be written as

$$a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \cdots + b_{ij}\beta_j, \tag{1.2}$$

with $b_{ij} \in F$. Putting (1.2) into (1.1) we see k is a linear combination of the elements $\alpha_i\beta_j$. Next, suppose

$$c_{11}\alpha_1\beta_1 + \cdots + c_{1m}\alpha_1\beta_m + \cdots + c_{n1}\alpha_n\beta_1 + \cdots + c_{nm}\alpha_n\beta_m = 0,$$

for some $c_{ij} \in K$. This can be read as

$$(c_{11}\beta_1 + \cdots + c_{1m}\beta_m)\alpha_1 + \cdots + (c_{n1}\beta_1 + \cdots + c_{nm}\beta_m)\alpha_n = 0,$$

and since the α_is are linearly independent, we must have

$$c_{i1}\beta_1 + \cdots + c_{im}\beta_m = 0,$$

for each $i = 1, \ldots, n$. But since the β_is are linearly independent too, we must have $c_{i,j} = 0$ for $j = 1, \ldots, m$ and each $i = 1, \ldots, n$. □

Given a field extension L/K, we want an intermediate field extension of K that is contained in L. One such way is to consider a suitable polynomial $f(x) \in F[x]$ which cannot be factored within K but can be in L; suppose $\alpha \in L \setminus K$ is a root of $f(x)$. Then we can enlarge K to create a field $K[\alpha]$ which is the minimal field that contains K and α. More precisely, if we let $\mathscr{M}$ be the collection of all subfields that contain both K and α, then

$$K[\alpha] = \bigcap_{F \in \mathscr{M}} F.$$

It's easy to check that $K[\alpha]$ is indeed a subfield of L. A more constructive description of $K[\alpha]$ is obtained by considering the ring homomorphism $\varphi : K[x] \to K[\alpha]$ determined by sending $x \mapsto \alpha$. We let K' be the isomorphic image of $K[x]/\operatorname{Ker}(\varphi)$ in $K[\alpha]$. It's clear that K' a subfield of $K[\alpha]$ and since it contains both K and α, must be equal to $K[\alpha]$, i.e., $K[x]/\operatorname{Ker}(\varphi) \cong K[\alpha]$.

Now since $K[x]/\operatorname{Ker}(\varphi)$ is a field, $\operatorname{Ker}(\varphi)$ must be a maximal ideal of $K[x]$. Recall that since $K[x]$ is a PID, it must be the case that $\operatorname{Ker}(\varphi)$ is generated by an irreducible polynomial, i.e., $\operatorname{Ker}(\varphi) = (f(x))$ with $f(x)$ irreducible. By the definition of kernel, we then have $f(\alpha) = 0$, and the same is true for any $g(x) \in \operatorname{Ker}(\varphi) = (f(x))$. Since K is a field, we can choose $f(x)$ to be monic (i.e., its leading term has coefficient 1). We now have an explicit description of $K[\alpha] \cong K[x]/(f(x))$ as being the set of remainder classes of $K[x]$ under division by $f(x)$. Thus if $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, then

$$K[\alpha] = \{k_{d-1}\alpha^{d-1} + k_{d-2}\alpha^{d-2} + \cdots + k_0 \mid k_i \in K\}.$$

This description immediately shows that the d elements $\alpha^{d-1}, \alpha^{d-2}, \ldots, 1$ form a basis for $K[\alpha]$ over K and so $[K[\alpha] : K] = d$. The monic irreducible polynomial $f(x)$ with $f(\alpha) = 0$ is called the **minimal polynomial** of α and plays an important role in field theory.

Definition 1.5 (Integrality) Let A be a subring of a commutative ring B. Then an element $b \in B$ is *integral* over A if there exist $n \in \mathbb{Z}_{\geq 1}$ and $a_i \in A$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

In other words there exists a monic $p(x) \in A[x]$ such that $p(b) = 0$. The *integral closure* of A in B is the set of elements in B that are integral over A. Further, A is *integrally closed* if the integral closure of A in its field of fractions is again A.

We have this useful fact:

Proposition 1.6 *Every Unique Factorization Domain (UFD) is integrally closed.*

Proof. The proof is an emulation of the proof of the Rational Roots theorem. Let A be a UFD with field of fractions K. Suppose $\alpha \in K$ is integral over A, so that there exists $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that $f(\alpha) = 0$. Let $\alpha = r/s$ with $r, s \in A$ and, using unique factorization, cancel any common irreducibles in their factorizations. So, we have

$$r^n + s^n a_{n-1}r^{n-1} + \cdots + s^n a_0 = 0.$$

Since $s \mid s^n a_{n-1}r^{n-1} + \cdots + s^n a_0$, we must have $s \mid r^n$. But since s and r share no irreducibles, it must be the case that s is a unit in A, i.e., $\alpha \in A$. □

A very close concept, essentially interchangeable with integrality in the case of fields, is the following.

Definition 1.7 (Algebraic) Let A be a subring of a commutative ring B. Then an element $\alpha \in B$ is called *alegbraic* over A if there exists (not necessarily monic) $p(x) \in R[x]$ such that $p(\alpha) = 0$. If all elements of a field extension L/K are algebraic over K, then L is an *algebraic extension* of K.

We have a very useful connection between finite and algebraic extensions.

Proposition 1.8 *If L/K is a finite field extension, then L/K is also algebraic.*

Proof. Fix an element $\alpha \in L$ and let $n = [L : K]$. Then the $n + 1$ elements $\alpha^n, \alpha^{n-1}, \ldots, 1$ are linearly dependent and so there must exist $k_i \in K$, not all zero, such that

$$k_n\alpha^n + k_{n-1}\alpha^{n-1} + \cdots + k_0 = 0.$$

Let m be the maximum i with nonzero k_i. Then the monic polynomial

$$x^m + k_m^{-1}k_{m-1}x^{m-1} + \cdots + k_m^{-1}k_0$$

has α as a root. □

Recall that a finite integral domain is a field. The next result gives another instance of when even an infinite integral domain can be shown to be a field. Indeed, its proof is in the same spirit as the former result.

Lemma 1.9 *Let A is an integral domain containing a field K. If A is algebraic over K, then A is a field.*

Proof. Suppose $\beta \in A$ is nonzero. Since β is algebraic over K, the field $K[\beta]$ is finite-dimensional over K. Since $K[\beta]$ is an integral domain, the mapping $k \mapsto k\beta : K[\beta] \to K[\beta]$ is injective and by finite-dimensionality, is surjective too. Thus, there exists $\alpha \in K[\beta]$ such that $\alpha\beta = 1$, implying β has a mutliplicative inverse. Hence A is a field. □

We can also think about doing linear algebra with a finite field extension L/K. Two maps that arise from this viewpoint will be important in our study of algebraic number theory. Notice that for each element $l \in L$, the map $\phi_l : L \to L$ given by $\phi_l(\alpha) = l\alpha$ is a K-linear mapping:

$$\phi_l(k_1\alpha_1 + k_2\alpha_2) = l(k_1\alpha_1 + k_2\alpha_2) = k_1(l\alpha_1) + k_2(l\alpha_2) = k_1\phi_l(\alpha_1) + k_2\phi_l(\alpha_2),$$

for all $k_1, k_2 \in K$ and $\alpha_1, \alpha_2 \in L$. So, we can talk about the trace and determinant of ϕ_l, given by the trace and determinant of the matrix representation of ϕ_l with respect to any basis of L over K. The **trace** $\mathrm{Tr}(l)$ and **norm** $\mathrm{Nm}(l)$ of an element $l \in L/K$ is the trace and determinant of ϕ_l respectively. Fear not, we won't have to explicitly compute the norm by doing a determinant because we have a simple but beautiful relationship with the minimal polynomial.

Proposition 1.10 *Let L/K be a finite (separable) field extension of degree n. Suppose $\alpha \in L$ has a minimal polynomial over K with roots $\alpha_1, \alpha_2, \ldots, \alpha_m$ (so that $[K[\alpha] : K] = m$), then*

$$\mathrm{Tr}(\alpha) = r\sum_{i=1}^{m} \alpha_i \textit{ and } \mathrm{Nm}(\alpha) = \Big(\prod_{i=1}^{m} \alpha_i\Big)^r,$$

where $r = n/m$ is the degree $[L : K[\alpha]]$.

Proof. First suppose $L = K[\alpha]$ and let the minimal polynomial of α be $x^m + a_{m-1}x^{m-1} + \cdots + a_0$. We showed above that $1, \alpha, \ldots, \alpha^{m-1}$ form a basis for L over K and with respect to this basis,

$$\phi_\alpha = \begin{pmatrix} 0 & \ldots & 0 & -a_0 \\ 1 & \ldots & 0 & -a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & -a_{m-2} \\ 0 & \ldots & 1 & -a_{m-1} \end{pmatrix},$$

and so by Vieta's formula $\mathrm{Tr}(\alpha) = -a_{m-1} = \sum_{i=1}^m \alpha_i$ and $\mathrm{Nm}(\alpha) = (-1)^{m-1}(-a_0) = \prod_{i=1}^m \alpha_i$. For the general case, suppose $\beta_1, \beta_2, \ldots, \beta_r$ is a basis for $L/K[\alpha]$. Then the elements $\{\alpha^i \beta_j\}$ for $0 \leq i < m$ and $1 \leq j \leq r$ are a basis for L/K (cf. proof of Lemma 1.4) and so ϕ_α will just be composed of r copies along the diagonal of our previous ϕ_α. □

The trace pairing

$$(\alpha, \beta) \mapsto \mathrm{Tr}(\alpha\beta) : L \times L \to K,$$

gives us a K-bilinear map (linear in each of its slots, when the other is fixed) to K. It can be shown that for this mapping the **discriminant** defined as $\det(\mathrm{Tr}(e_i e_j))$, for some basis $e_1, \ldots, e_n$ of L/K, is nonzero.[1] This leads to a very nice consequence: suppose we have a general K-linear mapping $\phi : L \to K$ such that $\phi(e_i) = k_i$, so that for any $\alpha = \sum_{i=1}^n a_i e_i \in L$, we have $\phi(\alpha) = \sum_{i=1}^n a_i k_i$. We can then find an element $\beta = \sum_{i=1}^n b_i e_i \in L$ such that $\phi(\alpha) = \mathrm{Tr}(\alpha\beta)$ for all $\alpha \in L$, by solving the linear system

$$\begin{pmatrix} \mathrm{Tr}(e_1e_1) & \mathrm{Tr}(e_1e_2) & \ldots & \mathrm{Tr}(e_1e_n) \\ \mathrm{Tr}(e_2e_1) & \mathrm{Tr}(e_2e_2) & \ldots & \mathrm{Tr}(e_2e_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(e_ne_1) & \mathrm{Tr}(e_ne_2) & \ldots & \mathrm{Tr}(e_ne_n) \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{pmatrix},$$

because $\det(\mathrm{Tr}(e_i e_j)) \neq 0$. In other words, we have a surjective map from L to the dual space[2] L^* given by $\beta \mapsto (x \mapsto \mathrm{Tr}(x\beta))$. In fact, this is an isomorphism because the kernel of this mapping is just zero: for any $\beta \neq 0$, $\mathrm{Tr}(\beta^{-1}\beta) = \mathrm{Tr}(1) = \sum_{i=1}^n e_i \neq 0$. Now, L^* has a very nice basis: the functions $f_i : L \to K$ such that $f_i(e_j) = \delta_{ij}$.[3] By our isomorphism, we can therefore find elements $e_i' \in L$ such that $\mathrm{Tr}(e_i e_j') = \delta_{ij}$; because of this the elements e_i' have to be linearly independent and therefore form a basis too. Some refer to the e_i' as a kind of "dual basis".

1.2 Modules

Throughout this section we assume R is a commutative ring.

[1] Here we are still assuming L/K is a separable extension. Since all our work is eventaully over $\mathbb{Q}$, we don't have to worry about this. You may consult **??** to see what this condition means and why we need this in general. Also, we will not be proving that the discriminant is zero but encourage the interested reader to refer to **??**.

[2] i.e., the vector space of all K-linear mappings $L \to K$.

[3] δ_{ij} is the Kronecker delta, defined as 1 if $i = j$ and 0 otherwise.

Definition 1.11 (Module) An R*-module* is an additive abelian group M along with a mapping $(r, m) \mapsto rm : R \times M \to M$, so that the following hold for all $r_1, r_2 \in R, m_1, m_2 \in M$:

- $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$,
- $(r_1 + r_2)m_1 = r_1m + r_2m$,
- $(r_1r_2)m_1 = r_1(r_2m_1)$,
- $1m_1 = m_1$.

We can also talk about R-**submodules** N of an R-module M, which implies N is an R-module contained in M. Since modules have a group structure, a submodule N of a module M can be viewed as an abelian subgroup of M, so that we can form the group quotient M/N. M/N naturally inherits an R-module structure: $r(m + N) = rm + N$, for $r \in R, m \in M$, and is thus called a **quotient module**.

The generalization of linear mappings between vector spaces is the following.

Definition 1.12 (Module homomorphism) Let M and N be R-modules. A map $\phi : M \to N$ is a *module homomorphism* if

- $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in M$,
- $\phi(rx) = r\phi(x)$ for all $r \in R, x \in X$.

It shouldn't be too surprising that we can carry through all the isomorphism theorems from ring theory because, after all, rings can be viewed as special cases of modules. In particular, for a module homomorphism between R-modules $\phi : M \to N$, we have

$$M/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi),$$

where the kernel $\operatorname{Ker}(\phi) = \{m \in M : \phi(m) = 0\}$ and the image $\operatorname{Im}(\phi) = \{\phi(m) : m \in M\}$.

Definition 1.13 (Finitely generated module) Let M be an R-module. M is *finitely generated* if there exist elements $x_1, x_2, \ldots, x_n \in M, n \in \mathbb{Z}_{\geq 1}$ such that any element $m \in M$ can be written as an R-linear combination of the x_i's:

$$m = r_1x_1 + r_2x_2, \ldots, r_nx_n,\ r_i \in R.$$

Lemma 1.14 *Let S be a commutative ring integral over a subring R. Then for a finite set of elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$, $R[\alpha_1, \alpha_2, \ldots, \alpha_n]$[4] is finitely generated as an R-module.*

Proof. First we show that $R[\alpha_1]$ is finitely generated as an R-module. Since S is integral over R, we can write

$$\alpha_1^m + r_{m-1}\alpha_1^{m-1} + \cdots + r_0 = 0,$$

[4] Similar to $K[\alpha]$, $R[\alpha]$ denotes the ring $\{f(\alpha) : f(x) \in R[x]\}$. We can keep repeating this construction: $K[\alpha_1, \alpha_2] = K[\alpha_1][\alpha_2]$, and so on.

for some $r_i \in R, m \in \mathbb{Z}_{\geq 1}$. Then for an element in $R[\alpha_1]$, we can replace α_1^m and higher powers by an R-linear combination of $\alpha_{m-1}, \alpha_{m-2}, \dots, \alpha_0$, and therefore $R[\alpha_1]$ is finitely generated as an R-module.

Now, by the same reasoning $R[\alpha_1, \alpha_2]$ is finitely generated as an $R[\alpha_1]$-module. Suppose $s_0, \dots, s_{l-1}$ generate $R[\alpha_1, \alpha_2]$ over $R[\alpha_1]$. Then the ml elements $r_0 s_0, \dots, r_0 s_{l-1}, \dots, r_{m-1} s_0, \dots, r_{m-1} s_{l-1}$ generate $R[\alpha_1, \alpha_2]$ over R (this is reminiscent of the proof of Lemma 1.4). An induction then gives the required result. □

This next technical-looking lemma will be immensely useful at various points. Indeed, I suggest skipping it for now and to return to it when it's needed so as to place it in the correct context.

Lemma 1.15 *Let R be a commutative ring. Let M be a nonzero finitely generated R-module contained in a field, let $\mathfrak{a}$ be an ideal of R, and let ϕ be a R-module homomorphism $M \to M$ such that $\phi(M) \subseteq \mathfrak{a}M$. Then ϕ satisifies an equation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0,\ a_i \in \mathfrak{a}.$$

Proof. Let M be generated by the elements $x_1, \dots, x_n$. By the hypothesis, for each $i = 1, \dots, n$, $\phi(x_i) = \sum_{j=1}^n a_{ij} x_j$ for some $a_{ij} \in \mathfrak{a}$. So we have

$$\begin{pmatrix} \phi - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & \phi - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{22} & \dots & \phi - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Denote the matrix on the left by T. Then multiplying on the left by $\operatorname{Adj} T$, we we see that

$$\det(T) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

Since M is nonzero, at least one of the x_i's are nonzero and since M lies within a field, $\det(T) = 0$, which gives the required equation. □

Definition 1.16 (Noetherian module) A R-module M is *Noetherian* if all its submodules are finitely generated over R.

A useful equivalent definition is that a R-module is Noetherian if any infinite increasing sequence of submodules $N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$ of M eventually becomes constant: $N_k = N_{k+1}$ for large enough $k \in \mathbb{Z}$. It's not too difficult to prove the equivalence of these two definitions.

Noetherian modules are very much related to Noetherian rings. Indeed, a commutative ring R is Noetherian if and only if it is a Noetherian module over itself because all the R-submodules of R are precisely the ideals of R.

Lemma 1.17 *Let M be a Noetherian R-module and let N be an R-submodule of M. Then M/N is Noetherian.*

Proof. Just as for rings, the following correspondence for modules can be verified: the R-submodules of M/N are in bijection with the R-submodules of M that contain N. Therefore, suppose M' is an R-submodule of M containing N. We have to show that M'/N is finitely generated as an R-module. Since M is Noetherian, M' is finitely generated and so let $\alpha_1, \alpha_2, \ldots, \alpha_n \in M'$ generate M' over R. Then $\alpha_1 + N, \alpha_2 + N, \ldots, \alpha_n + N \in M'/N$ generate M'/N over R. □

Proposition 1.18 *Let R be Noetherian. Then every finitely generated R-module is Noetherian.*

Proof. Let M be a finitely generated R-module with a generator set $\alpha_1, \alpha_2, \ldots, \alpha_n$. Since R is Noetherian, the direct product R^n viewed as an R-module is Noetherian. Then, let $\phi : R^n \to M$ be the module homomorphism given by $(r_1, r_2, \ldots, r_n) \mapsto r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n$. Since M is finitely generated over R by the α_i's, ϕ is surjective on M. Therefore, we have an isomorphism of R-modules, $R^n / \operatorname{Ker}(\phi) \cong M$. By Lemma 1.17, $R^n / \operatorname{Ker}(\phi)$ is Noetherian and thus M is Noetherian. □

2 Algebraic Number Theory

The goal of this section is to give a rapid and reasonably complete introduction to the parts of algebraic number theory relevant to its connections with graph theory.

2.1 Ring of Integers

Definition 2.1 (Number field) A *number field* is a finite field extension of $\mathbb{Q}$.

Important examples of number fields are **quadratic number fields** which are of form $\mathbb{Q}[\sqrt{d}]$ with d a squarefree integer; they all have degree 2 over $\mathbb{Q}$. Another favorite family of number fields is **cyclotomic fields** having the form $\mathbb{Q}[\zeta_m]$ with ζ_m a complex primitive mth root of unity (so $\operatorname{Im}(\zeta_m) \neq 0$, $\zeta_m^m = 1$, and $\zeta_m^k \neq 1$ for any $1 \leq k < m$); they have degree m over $\mathbb{Q}$.

We hope to study a subring of a number field K that plays a similar role to that of the integers $\mathbb{Z}$ in $\mathbb{Q}$. Particularly, we want a subring that emulates the elegant arithmetic of $\mathbb{Z}$.

Definition 2.2 (Ring of integers) Let K be a number field. The *ring of integers* $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.

There are many preliminary indications that this is the correct definition for $\mathcal{O}_K$. One is that K is the field of fractions of $\mathcal{O}_K$ (we prove this shortly) just like $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. But we have not yet verified that $\mathcal{O}_K$ is indeed a ring. Let's do that.

Proposition 2.3 *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

Proof. We have to show that $\mathcal{O}_K$ is closed under addition and multiplication. Fix $\alpha, \beta \in \mathcal{O}_K$. Then consider the $\mathbb{Z}$-module $M = \mathbb{Z}[\alpha, \beta] \subseteq K$. Clearly, $(\alpha + \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$. So if we can show that M is a finitely generated $\mathbb{Z}$-module, then in Lemma 1.15 we can take $R = \mathfrak{a} = \mathbb{Z}$ and ϕ as the homomorphisms $x \mapsto (\alpha + \beta)x$ and $x \mapsto (\alpha\beta)x$ to conclude closure.

Let $f(x), g(x) \in \mathbb{Z}[x]$ be the monic polynomials that are satisfied by α, β respectively. Let $m = \deg f$ and $n = \deg g$. Let M' be the $\mathbb{Z}$-submodule of M that is generated by the finite elements $\alpha^i\beta^j$ for $0 \leq i < m$ and $0 \leq j < n$. We show that $M = M'$ by showing $\alpha^I\beta^J \in M'$ for all $I, J \in \mathbb{Z}_{\geq 0}$. We can write

$$x^I = f(x)q_1(x) + r_1(x), x^J = g(x)q_2(x) + r_2(x),$$

with $q_i(x) \in \mathbb{Z}[x]$ and $\deg r_1 < m, \deg r_2 < n$. Then

$$\alpha^I = r_1(\alpha), \beta^J = r_2(\beta),$$

and so $\alpha^I\beta^J = r_1(\alpha)r_2(\beta) \in M'$. □

Proposition 2.4 *Let K be a number field. If $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}(\alpha), \mathrm{Nm}(\alpha) \in \mathbb{Z}$.*

Proof. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$. By Proposition 1.10, it suffices to show that $p(x)$ has coefficients in $\mathbb{Z}$. Since $\alpha \in \mathcal{O}_K$, there exists a relation

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0,$$

with $a_i \in \mathbb{Z}$. Looking back at our construction of $K[\alpha]$, its clear that if α' is another root of $p(x)$, then $K[\alpha] \cong K[\alpha']$ under the isomorphism σ determined by $\alpha \mapsto \alpha'$. Therefore,

$$0 = \sigma(\alpha)^m + a_{m-1}\sigma(\alpha)^{m-1} + \cdots + a_0 = \alpha'^m + a_{m-1}\alpha'^{m-1} + \cdots + a_0,$$

showing that α' is also integral over $\mathbb{Z}$. Thus, since the integral closure of $\mathbb{Z}$ in any field is a ring (the proof is virtually the same as above), the coefficients of $p(x)$ are also integral over $\mathbb{Z}$. But they also belong to $\mathbb{Q}$ (by definition of minimal polynomial), and since $\mathbb{Z}$ is integrally closed (Proposition 1.6), we conclude they belong to $\mathbb{Z}$. □

Proposition 2.5 *Let K be a number field. Then K is the field of fractions of $\mathcal{O}_K$.*

Proof. Fix an element $k \in K$. We want to show that there exists an element $\alpha \in \mathcal{O}_K$ such that $\alpha k \in \mathcal{O}_K$. Since K is a finite extension of $\mathbb{Q}$, by Proposition 1.8, k is algebraic over $\mathbb{Q}$ and so we have

$$k^n + q_{n-1}k^{n-1} + \cdots + q_0 = 0,$$

for some $q_i \in \mathbb{Q}$. Let the common denominator of the rationals q_i be α. Then multiplying through by α^n, we see

$$(\alpha k)^n + (q_{n-1}\alpha)(\alpha k)^{n-1} + \cdots + \alpha^n q_0 = 0,$$

and so αd is integral over $\mathbb{Z}$, i.e., $\alpha d \in \mathcal{O}_K$. □

In the proof above, because α is an integer, we actually have the stronger result that every element of K can be written as β/n with $\beta \in \mathcal{O}_K$ and $n \in \mathbb{Z}$.

Since we are asserting that in the context of arithmetic $\mathcal{O}_K$ is the correct generalization of $\mathbb{Z}$, a natural question is: does the Fundamental Theorem of Artihmetic (FTA) hold in $\mathcal{O}_K$? Or some might prefer the rephrasing: is $\mathcal{O}_K$ a UFD? In general it isn't, which is the main reason why Fermat's Last theorem is so hard. The classic example for the failure of FTA is $\mathbb{Q}[\sqrt{-5}]$: 6 can be factored into irreducibles as both $2 \cdot 3$ and $(1 - \sqrt{-5})(1 + \sqrt{-5})$. We can recover FTA by considering the set of ideals in $\mathcal{O}_K$, and now we build up the theory required to prove this fact.

2.2 Dedekind domains

We come to the algebraic structure central to understanding $\mathcal{O}_K$, but first consider a local version of it.

Definition 2.6 (Discrete valuation ring) A principal ideal domain (PID) is a *discrete valuation ring* if it has a unique non-zero prime ideal. For a discrete valuation ring A, we denote its nonzero prime ideal by $\mathfrak{m}(A)$.

Suppose $\mathfrak{m}(A) = (\pi)$. Then π has to be irreducible because otherwise we would have a prime ideal that properly contained $\mathfrak{m}$. Further π is an associate of any other irreducible element in A, and thus is effectively the only irreducible in A; it's called the **uniformizer** of A. Since any nonzero element $a \in A$ can be written as $a = \pi^n u$ for some unit $u \in A$ and $n \in \mathbb{Z}_{\geq 0}$, every nonzero ideal of A is of the form $(\pi^n) = \mathfrak{m}^n$ for a unique n. Therefore we already have a very simple FTA for the ideals in DVRs, and so if we are able to show, loosely speaking, that $\mathcal{O}_K$ (more generally, a Dedekind domain) can be constructed by glueing together DVRs, then we can lift the FTA to the ideals of $\mathcal{O}_K$.

An example of a DVR is the subring $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ for some prime $p \in \mathbb{Z}$ of elements r/s such that $p \nmid s$. The prime ideal $\mathfrak{m}(\mathbb{Z}_{(p)})$ is (p) and the units of $\mathbb{Z}_{(p)}$ are the elements a/b with $p \nmid a$ (and by definition $p \nmid b$).

An analytic example is the following. Let X be a Riemann surface and $p \in X$. Then the ring $\mathfrak{H}_p$ of holomorphic functions in any neighborhood of p is a DVR. $\mathfrak{H}_p$ is isomorphic to the subring $\mathbb{C}\{x\}$ of convergent series in the ring $\mathbb{C}[[x]]$ of formal power series with coefficients in $\mathbb{C}$. Its unique prime ideal is the ideal of convergent power series $\sum a_n z^n$ such that $a_0 \neq 0$.

Proposition 2.7 *An integral domain A is a discrete valuation ring if and only if*

1. *A is Noetherian,*
2. *A is integrally closed, and*
3. *A has exactly one nonzero prime ideal.*

Proof. The forward direction is clear. Indeed, the first and third implications follow directly from the definition of a DVR and the second implication follows from Proposition 1.6 because a DVR is a PID and hence a UFD. So, suppose A is an integral domain satisfying the three conditions. We have to show A is a PID.

Fix a nonzero nonunit $c \in A$ and let $M = A/(c)$. The key idea is to consider, for each nonzero $m \in M$, the *annihilator* $\operatorname{Ann}(m)$ of m defined as

$$\operatorname{Ann}(m) = \{a \in A \mid am = 0\}.$$

Note that $\operatorname{Ann}(m)$ is a proper ideal of A. Since A is Noetherian we can choose an $m \in M$ such that $\operatorname{Ann}(m)$ is maximal among ideals of this form (i.e., there exists no nonzero $m' \in M$ such that $\operatorname{Ann}(m) \subsetneq \operatorname{Ann}(m')$). Let $m = b + (c)$ and $\mathfrak{p} = \operatorname{Ann}(b + (c))$.

We first show that $\mathfrak{p}$ is prime by supposing it's not. Then there exist $x, y \in A$ such that $xy \in \mathfrak{p}$ but $x \notin \mathfrak{p}, y \notin \mathfrak{p}$. Then clearly $\mathfrak{p} \subseteq \operatorname{Ann}(yb + (c))$ and $x \in \operatorname{Ann}(yb + (c))$, contradicting the maximality of $\mathfrak{p}$ among annhilators.

Next, note $b/c \notin A$ because otherwise $b \in (c)$, contradicting $b + (c) = m \neq 0$. We argue that $\mathfrak{p} = (c/b)$. By construction $\mathfrak{p}b \subseteq (c)$, so that $\mathfrak{p} \cdot b/c \subseteq A$. If $\mathfrak{p} \cdot b/c \subseteq \mathfrak{p}$, then by Lemma 1.15 (taking $M = \mathfrak{p}, \mathfrak{a} = A, \phi(m) = m \cdot b/c$) b/c is integral over A. Condition (b) then implies $b/c \in A$, which we showed isn't possible. So by condition (c), $\mathfrak{p} \cdot b/c = A$, i.e., $\mathfrak{p} = (c/b)$. Let $\pi = c/b$.

Finally, let $\mathfrak{a}$ be an ideal of A. In the field of fractions of A, consider the increasing sequence of ideals

$$\mathfrak{a} \subseteq \pi^{-1}\mathfrak{a} \subseteq \pi^{-2}\mathfrak{a} \subseteq \ldots.$$

If this sequence is contained in A, then because A is Noetherian, there exists $r \in \mathbb{Z}_{\geq 1}$ such that $\pi^{-r-1}\mathfrak{a} = \pi^{-r}\mathfrak{a}$, which by Lemma 1.15 implies that $\pi^{-1} \in A$, a contradiction. Therefore, there exists an $m \in \mathbb{Z}$ such that $\pi^{-m}\mathfrak{a} \subseteq A$ but $\pi^{-m-1}\mathfrak{a} \nsubseteq A$. Then $\pi^{-m}\mathfrak{a} \nsubseteq \mathfrak{p}$ and so $\pi^{-m}\mathfrak{a} = A$, i.e., $\mathfrak{a} = (\pi^m)$. □

Definition 2.8 (Dedekind domain) An integral domain A is a *Dedekind domain* if

- A is Noetherian,
- A is integrally closed, and
- every nonzero prime ideal is maximal.

Note that $\mathbb{Z}$ is a Dedekind domain: being a PID, it is Noetherian and every nonzero prime ideal is maximal; by Proposition 1.6 it is integrally closed.

A **local ring** is a ring with exactly one maximal ideal; DVRs are local rings. Proposition 2.7 tells us that a local Dedekind domain is a DVR. We will show $\mathcal{O}_K$ is actually a Dedekind domain, but only after proving a FTA for the ideals of a general Dedekind domain. The precise statment is this:

Theorem 2.9 (FTA for Dedekind domains) *Let A be a Dedekind domain. Every proper nonzero ideal $\mathfrak{a}$ of A can be written as*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k},$$

with the $\mathfrak{p}_i$ distinct prime ideals and $r_i \in \mathbb{Z}_{>0}$. Furthermore, this expression is unique.

We break the proof into a series of smaller lemmas, with the first goal being to show that the localisation of a Dedekind domain at a prime ideal is a DVR.

A set $S \subseteq A$ is **multiplicative** if $0 \notin S$, $1 \in S$ and S is closed under multiplication. The multiplicative subset that will be important for us is $S = A - \mathfrak{p}$, for a nonzero prime ideal $\mathfrak{p}$ of A. The ring $A_{\mathfrak{p}} = S^{-1}A$ is called the **localization** of A at $\mathfrak{p}$.

Proposition 2.10 *Let S be a multiplicative subset of a Dedekind domain A. Then $S^{-1}A$ is a Dedekind domain.*

Proof. We first establish a correspondence between the prime ideals of A and $S^{-1}A$. We show the map $\mathfrak{p} \mapsto \mathfrak{p}^e := \mathfrak{p} \cdot S^{-1}A$ is a bijection between the prime ideals of A such that $\mathfrak{p} \cap S = \varnothing$ and the prime ideals of $S^{-1}A$.[5] Suppose $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{p} \cap S = \varnothing$ and $xy \in \mathfrak{p}^e$. Then we can write $xy = pa/s$ for some $p \in \mathfrak{p}, a \in A, s \in S$, and so $sxy \in \mathfrak{p}$. Since $s \notin \mathfrak{p}$, we must then have $xy \in \mathfrak{p}$, and so either x or y is in $\mathfrak{p} \subseteq \mathfrak{p}^e$. Therefore $\mathfrak{p}^e$ is indeed prime. A similar argument shows that the mapping $\mathfrak{p} \mapsto \mathfrak{p}^c := \mathfrak{p} \cap A$ from the prime ideals of $S^{-1}A$ to the prime ideals of A that don't meet S is an inverse of $\mathfrak{p} \mapsto \mathfrak{p}^e$.

[5] The notation $\mathfrak{p}^e$ is commonly used to denote the *extension* of an ideal in a larger ring. The notation $\mathfrak{p}^c$ denotes the *contraction* of an ideal in a smaller ring.

The condition that every nonzero prime ideal is maximal is equivalent to there being no larger prime ideal between any prime ideal $\mathfrak{p}$ and the entire ring $S^{-1}A$. Indeed, since $\mathfrak{p}^c$ is a prime ideal of A and there is no prime ideal between $\mathfrak{p}^c$ and A, there can be no prime ideal between $\mathfrak{p}$ and $S^{-1}A$.

Next, suppose $\mathfrak{a}$ is an ideal of $S^{-1}A$. Then $\mathfrak{a} = S^{-1} \cdot \mathfrak{a}^c$ and so a set of finite generators for $\mathfrak{a}^c$ is also a finite set of generators for $\mathfrak{a}$. Therefore $S^{-1}A$ is Noetherian.

Finally, suppose α in the field of fractions of $S^{-1}A$ is integral over $S^{-1}A$. Then we have

$$\alpha^n + \alpha^{n-1}b_{n-1} + \cdots + b_0 = 0,$$

for some $b_i \in S^{-1}A$. We can find $s_i \in S$ such that $s_i b_i \in A$, and so letting $s = s_0 s_1 \ldots s_{n-1}$,

$$(s\alpha)^n + (s\alpha)^{n-1} s b_{n-1} + \cdots + s^n b_0 = 0.$$

This shows $s\alpha$ is integral over A and thus $s\alpha \in A$. Hence $\alpha \in S^{-1}A$. □

Proposition 2.11 *A Noetherian integral domain A is a Dedekind domain if and only if $A_{\mathfrak{p}}$ is a DVR for every nonzero prime ideal $\mathfrak{p}$ of A.*

Proof. Note that $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}^e$ and so the forward direction is proved in Proposition 2.10 (since a local Dedekind domain is a DVR). For the reverse direction, we have to show every prime ideal of A is maximal and A is integrally closed. First suppose $\mathfrak{p}$ is a nonzero prime ideal but is properly contained in a larger maximal ideal $\mathfrak{m}$. Then the extension $\mathfrak{p}^e$ of $\mathfrak{p}$ in $A_{\mathfrak{m}}$ is prime and is properly contained in the prime ideal $\mathfrak{m}^e$, contradicting that $A_{\mathfrak{m}}$ is a DVR.

Next suppose α is an element of the field of fractions of A that is integral over A. Since $A \subseteq A_{\mathfrak{p}}$ for each nonzero prime ideal $\mathfrak{p}$, α is integral over each $A_{\mathfrak{p}}$ and since $A_{\mathfrak{p}}$ is a DVR, $\alpha \in A_{\mathfrak{p}}$. Therefore, there exists an $s \in A - \mathfrak{p}$ such that $s\alpha \in A$. Let $\mathfrak{a}$ be the set of elements $a \in A$ such that $a\alpha \in A$. Notice $\mathfrak{a}$ is an ideal of A and we just showed it contains an element of $A - \mathfrak{p}$ for every nonzero prime ideal. Thus $\mathfrak{a} = A$, and so $1 \in \mathfrak{a}$. Hence $x \in A$. □

We now proceed to prove Theorem 2.9. We need three intuitively plausible lemmas from commutative algebra.

Lemma 2.12 *Let A be a Noetherian ring. Then every nonzero ideal of A contains a product of nonzero prime ideals.*

Proof. Suppose not. Since A is Noetherian, we can choose a maximal $\mathfrak{a}$ among all ideals which do not satisfy the claimed property. Since $\mathfrak{a}$ cannot be a prime ideal, there exist $x, y \in A$ such that $xy \in \mathfrak{a}$ but neither $x \in \mathfrak{a}$ nor $y \in \mathfrak{a}$. Then consider the two ideals $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$. Since $\mathfrak{a}$ is properly contained in both $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$, by the maximal property of $\mathfrak{a}$, $(x) + \mathfrak{a}$

and $(y) + \mathfrak{a}$ contain a product of nonzero prime ideals. But then the product of these products is contained in $((x) + \mathfrak{a})((y) + \mathfrak{a}) \subseteq \mathfrak{a}$, a contradiction. □

Recall that in a ring A, two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime if $\mathfrak{a} + \mathfrak{b} = A$.

Lemma 2.13 *Let A be a commutative ring with relatively prime ideals $\mathfrak{a}$ and $\mathfrak{b}$. Then $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are relatively prime for all $m, n \in \mathbb{Z}_{\geq 0}$.*

Proof. First we show that a commutative ring R (with $1 \neq 0$) has at least one maximal ideal. Let S be the set the of ideals in R not equal to R. Then ordering S by set inclusion, if $(\mathfrak{i}_\alpha)$ is a chain of ideals in S, then $\bigcup_\alpha \mathfrak{i}_\alpha$ is an ideal of A too which is an upper bound of $(\mathfrak{i}_\alpha)$. So, by Zorn's lemma[6], S contains a maximal element. Using this result, we can deduce than any ideal $\mathfrak{a} \neq A$ is contained in a maximal ideal of A: $A/\mathfrak{a}$ has a maximal ideal, which corresponds to maximal ideal of A that contains $\mathfrak{a}$.

Returning to the lemma, suppose it's false. Then $\mathfrak{a}^m + \mathfrak{b}^n$ is contained in a maximal ideal $\mathfrak{p}$. If $a \in \mathfrak{a}$, then $a^m \in \mathfrak{a}^m \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, this means $a \in \mathfrak{p}$, i.e., $\mathfrak{a} \subseteq \mathfrak{p}$. Similarly, $\mathfrak{b} \subseteq \mathfrak{p}$. Since $\mathfrak{a} + \mathfrak{b} = A$, this contradicts that $\mathfrak{p}$ is prime. □

Lemma 2.14 *Let $\mathfrak{p}$ be a maximal ideal of an integral domain A and let $\mathfrak{q} = \mathfrak{p}^e$ be the extension of $\mathfrak{p}$ in $A_\mathfrak{p}$, i.e, $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$. Then the mapping*

$$a + \mathfrak{p}^m \mapsto a + \mathfrak{q}^m : A/\mathfrak{p}^m \to A_\mathfrak{p}/\mathfrak{q}^m,$$

is an isomorphism for all $m \in \mathbb{Z}_{\geq 0}$.

Proof. The mapping is clearly a homomorphism. To show the mapping is injective, we show its kernel is trivial, i.e., $\mathfrak{q}^m \cap A = \mathfrak{p}^m$. Fix an element $a \in \mathfrak{q}^m \cap A$. Then $a = p/s$, where $p \in \mathfrak{p}^m, s \in S = A - \mathfrak{p}$, and so $sa \in \mathfrak{p}^m$. Now $\mathfrak{p}$ is the only maximal ideal containing $\mathfrak{p}^m$ (since if $\mathfrak{p}^m \subseteq \mathfrak{m}$ then $\mathfrak{p} \subseteq \mathfrak{m}$). Therefore $\mathfrak{p}/\mathfrak{p}^m$ is the only maximal ideal of $A/\mathfrak{p}^m$. Since $s \notin \mathfrak{p}$, it follows that s is a unit in $A/\mathfrak{p}^m$ and so $sa = 0 \bmod \mathfrak{p}^m$ implies $a = 0 \bmod \mathfrak{p}^m$, i.e., $a \in \mathfrak{p}^m$.

To show the mapping is surjective, fix $a/s \in A_\mathfrak{p}$. Then, since $s \notin \mathfrak{p}$ and $\mathfrak{p}$ is maximal, (s) and $\mathfrak{p}$ are relatively prime. By Lemma 2.13, (s) and $\mathfrak{p}^m$ are also relatively prime. Therefore, there is $b \in A, p \in \mathfrak{p}^m$ such that $sb + p = 1$. This implies $sb = 1 \bmod \mathfrak{q}^m$, i.e., $b = s^{-1} \bmod \mathfrak{q}^m$, and so $ab = a/s \bmod \mathfrak{q}^m$. □

We are now ready to prove Theorem 2.9. We will make repeated use of Proposition 2.11 that guarantees the localisation $A_\mathfrak{p}$ at a nonzero prime ideal $\mathfrak{p}$ of A is a DVR.

[6] Zorn's lemma states that given a non-empty poset S, if every chain in S has an upper bound, then S has a maximal element. A *poset* is a set with a relation $\leq$ which is transitive, reflexive and antisymmetric, i.e., if $a \leq b$ and $b \leq a$ then $a = b$. A *chain* in a poset is a set in which any pair of elements can be compared via $\leq$.

Proof. Let $\mathfrak{a}$ be a nonzero ideal of a Dedekind domain A. By Lemma 2.12, $\mathfrak{a}$ contains a product of nonzero prime ideals

$$\mathfrak{b} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots\mathfrak{p}_k^{r_k},$$

for distinct $\mathfrak{p}_\mathfrak{i}$ and $r_i \in \mathbb{Z}_{>0}$. Then by the Chinese Remainder theorem[7] and Lemma 2.14,

$$A/\mathfrak{b} \cong A/\mathfrak{p}_1^{r_1} \times A/\mathfrak{p}_2^{r_2} \times \cdots \times A/\mathfrak{p}_k^{r_k} \cong A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times A_{\mathfrak{p}_2}/\mathfrak{q}_2^{r_2} \times \cdots \times A_{\mathfrak{p}_k}/\mathfrak{q}^{r_k},$$

where $\mathfrak{q}_i$ is the extension of $\mathfrak{p}_i$ in $A_{\mathfrak{p}_i}$, and by Proposition 2.11 it is the maximal ideal of the DVR $A_\mathfrak{p}$. Now, recall that the ideal of a direct product of rings is a direct product of ideals in those rings. Therefore, since $\mathfrak{a}/\mathfrak{b}$ is an ideal of $A/\mathfrak{b}$,

$$\mathfrak{a}/\mathfrak{b} \cong \mathfrak{i}_1/\mathfrak{q}_1^{r_1} \times \mathfrak{i}_2/\mathfrak{q}_2^{r_2} \times \cdots \times \mathfrak{i}_k/\mathfrak{q}^{r_k},$$

where $\mathfrak{i}_j$ is an ideal of $A_{\mathfrak{p}_j}$ containing $\mathfrak{q}_j^{r_j}$. Since $A_{\mathfrak{p}_j}$ is a DVR, $\mathfrak{i}_j$ must be of the form $\mathfrak{q}_j^{s_j}$ for $s_j \in \mathbb{Z}_{\geq 0}$. Further, for $\mathfrak{i}_j$ to contain $\mathfrak{q}_j^{r_j}$, we must have $s_j \leq r_j$. Therefore,

$$\mathfrak{a}/\mathfrak{b} \cong \mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \mathfrak{q}_2^{s_2}/\mathfrak{q}_2^{r_2} \times \cdots \times \mathfrak{q}_k^{s_k}/\mathfrak{q}^{r_k},$$

for some nonnegative $s_j \leq r_j$. However, note also that

$$\mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}/\mathfrak{b} \cong \mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \mathfrak{q}_2^{s_2}/\mathfrak{q}_2^{r_2} \times \cdots \times \mathfrak{q}_k^{s_k}/\mathfrak{q}^{r_k}.$$

(A way to see this is

$$\mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}/\mathfrak{b} \cong \mathfrak{p}_1^{s_1}/\mathfrak{p}_1^{r_1} \times \mathfrak{p}_2^{s_2}/\mathfrak{p}_2^{r_2} \times \cdots \times \mathfrak{p}_k^{s_k}/\mathfrak{p}_k^{r_k},$$

by the Chinese Remainder theorem and the fact that $\mathfrak{p}_i^{s_i} + \mathfrak{p}_j^{r_j} = A$ for $i \neq j$. Then apply Lemma 2.14.) Thus we have an equality of ideals in $A/\mathfrak{b}$,

$$\mathfrak{a}/\mathfrak{b} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}/\mathfrak{b}.$$

Since both $\mathfrak{a}$ and $\mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}$ contain $\mathfrak{b}$, and there is a $1-1$ correspondence between ideals of $A/\mathfrak{b}$ and ideals of A containing $\mathfrak{b}$, we have

$$\mathfrak{a} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}.$$

To show uniqueness of this expression, suppose

$$\mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2}\dots\mathfrak{p}_k^{t_k} = \mathfrak{a} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k},$$

allowing some t_i's and s_j's to be zero if needed. Then because $A_{\mathfrak{p}_1}$ is a DVR with the unique maximal ideal $\mathfrak{q}_1$, we have

$$\mathfrak{a}A_{\mathfrak{p}_1} = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2}\dots\mathfrak{p}_k^{t_k}A_{\mathfrak{p}_1} = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2}\dots\mathfrak{p}_{k-1}^{t_{k-1}}A_{\mathfrak{p}_1} = \cdots = \mathfrak{p}_1^{t_1}A_{\mathfrak{p}_1} = \mathfrak{q}_1^{t_1}.$$

[7] The CRT for a ring R states that if $\mathfrak{i}_1, \mathfrak{i}_2, \dots, \mathfrak{i}_k$ are pairwise relatively prime ideals, then $\mathfrak{i}_1\mathfrak{i}_2\dots\mathfrak{i}_k = \mathfrak{i}_1 \cap \mathfrak{i}_2 \cap \cdots \cap \mathfrak{i}_k$ and so by the Isomorphism theorem $R/(\mathfrak{i}_1\mathfrak{i}_2\dots\mathfrak{i}_k) \cong R/\mathfrak{i}_1 \times R/\mathfrak{i}_2 \times \cdots \times R/\mathfrak{i}_k$.

Similarly,

$$\mathfrak{a}A_{\mathfrak{p}_1} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k}A_{\mathfrak{p}_1} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_{k-1}^{s_{k-1}}A_{\mathfrak{p}_1} = \dots = \mathfrak{p}_1^{s_1}A_{\mathfrak{p}_1} = \mathfrak{q}_1^{s_1}.$$

Thus, $\mathfrak{q}_1^{t_1} = \mathfrak{q}_1^{s_1}$ and so $t_1 = s_1$ (recall, a DVR is a UFD). The same argument shows $t_j = s_j$ for all other j. □

In a PID, we have the useful fact that for two ideals $\mathfrak{a} \subseteq \mathfrak{b}$ if and only if $\mathfrak{b} \mid \mathfrak{a}$. In the proof of this, we actually don't need the full force of unique factorization afforded in a UFD but only unique factorization for the ideals and the fact that ideals are principal. In Dedekind domains, ideals need not be principal, but we don't lose this property precisely because a Dedekind domain is locally a DVR, a very special PID.

Corollary 2.15 ("To contain is to divide") *Let A be a Dedekind domain and let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals. Then $\mathfrak{a} \subseteq \mathfrak{b}$ if and only if $\mathfrak{b} \mid \mathfrak{a}$.*

Proof. The reverse direction is quite straightforward and is indeed true in any commutative ring. If $\mathfrak{b} \mid \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$. So any element $a \in \mathfrak{a}$ is of the form $\sum_{i=1}^n b_i c_i$ for some $b_i \in \mathfrak{b}, c_i \in \mathfrak{c}$, and $n \in \mathbb{Z}_{\geq 1}$. Since $\sum_{i=1}^n b_i c_i \in \mathfrak{b}$, it follows $\mathfrak{a} \subseteq \mathfrak{b}$.

Now suppose $\mathfrak{a} \subseteq \mathfrak{b}$. Let the prime ideal factorizations of $\mathfrak{a}$ and $\mathfrak{b}$ be

$$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots\mathfrak{p}_m^{r_m}, \mathfrak{b} = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_m^{s_m},$$

for distinct prime ideals $\mathfrak{p}_i$ and some $r_i, s_i \in \mathbb{Z}_{\geq 0}$. Then we have to show that $s_i \leq r_i$ for all i. Localising to $A_{\mathfrak{p}_i}$, we see

$$\mathfrak{a}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{r_i}A_{\mathfrak{p}_i} = \mathfrak{q}_i^{r_i} \text{ and } \mathfrak{b}A_{\mathfrak{p}_i} = \mathfrak{p}_i^{s_i}A_{\mathfrak{p}_i} = \mathfrak{q}_i^{s_i}.$$

Since $\mathfrak{a} \subseteq \mathfrak{b}$, it follows $\mathfrak{q}_i^{r_i} \subseteq \mathfrak{q}_i^{s_i}$, and so $s_i \leq r_i$. □

Another interesting application of unique factorization of ideals is the following. Since, by definition, Dedekind domains are Noetherian, it isn't too much of a surprise but still a very handy fact to have.

Corollary 2.16 *Let A be a Dedekind domain. Then every nonzero ideal of A can be generated by two elements of A.*

Proof. Let $\mathfrak{a}$ be a nonzero ideal of A. Fix a nonzero $\alpha \in \mathfrak{a}$. Let the prime ideal factorizations of $\mathfrak{a}$ and (α) be

$$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots\mathfrak{p}_k^{r_k} \text{ and } (\alpha) = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\dots\mathfrak{p}_k^{s_k},$$

with distinct prime ideals $\mathfrak{p}_i$ and $r_i, s_i \in \mathbb{Z}_{\geq 0}$. Since $\alpha \in \mathfrak{a}$, $(\alpha) \subseteq \mathfrak{a}$ and so by "to contain is to divide", $r_i \leq s_i$ for all i. We want to construct a $\beta \in A$ such that $(\alpha) + (\beta) = \mathfrak{a}$. This implies that the smallest ideal containing α and β is $\mathfrak{a}$, and so the prime ideal factorization of (β) has the form

$$(\beta) = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots\mathfrak{p}_k^{r_k}\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_l,$$

for some prime ideals $\mathfrak{q}_i$ distinct from the $\mathfrak{p}_i$'s. In fact, note that any principal ideal having the above form of prime ideal factorization will work. With this in mind, for each i fix a $\beta_i \in \mathfrak{p}_i^{r_i} \setminus \mathfrak{p}_i^{r_i+1}$. Then, since by the Chinese Remainder theorem

$$A/\mathfrak{p}_1^{r_1+1}\mathfrak{p}_2^{r_2+1}\dots\mathfrak{p}_k^{r_k+1} \cong A/\mathfrak{p}_1^{r_1+1} \times A/\mathfrak{p}_2^{r_2+1} \times \dots \times A/\mathfrak{p}_k^{r_k+1},$$

there exists $\beta \in A$ such that $\beta \mapsto (\beta_1 + \mathfrak{p}_1^{r_1+1}, \beta_2 + \mathfrak{p}_1^{r_2+1}, \dots, \beta_k + \mathfrak{p}_1^{r_k+1})$. So, by construction $\beta \in \mathfrak{p}_i^{r_i} \setminus \mathfrak{p}_i^{r_i+1}$ for all i, and hence β has the required prime ideal factorization ("to contain is to divide"!). Thus $\mathfrak{a} = (\alpha, \beta)$. □

Now, we come to the proof that $\mathcal{O}_K$ is a Dedekind domain. We prove the more general:

Theorem 2.17 *Let A be a Dedekind domain with field of fractions F having characteristic 0 and let K be a finite extension of F. Let B be the integral closure of A in K. Then B is a Dedekind domain.*

So taking $A = \mathbb{Z}, F = \mathbb{Q}$, $K =$ number field, $B = \mathcal{O}_K$, we will have shown $\mathcal{O}_K$ is a Dedekind domain.

Proof.

- *B is integrally closed:* We can check by an argument virtually same as that of Proposition 2.5, that K is the field of fractions of B. So let C be the integral closure of B in K; we have to show $C = B$. If we can show that C is also integral over A, then we would have that $C \subseteq B$, and since $B \subseteq C$, we would have $C = B$. Let $\alpha \in C$. Then we have

  $$\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_0 = 0,$$

  for some $b_i \in B$. Let $B' = A[b_{n-1}, b_{n-2}, \dots, b_0]$. By Lemma 1.14, B' is finitely generated as an A-module. Since α is integral over B', again by Lemma 1.14, $B'[\alpha]$ is finitely generated as a B'-module and hence as an A-module too (cf. proof of 1.14). Since, $\alpha \cdot B'[\alpha] \subseteq B'[\alpha]$, by Lemma 1.15, α is integral over A. Hence $\alpha \in B$, and so $C \subseteq B$.

- *B is Noetherian:* The key idea is to show B is contained in a finitely generated A-module M. Suppose we have shown this. Then by Proposition 1.18, M is a Noetherian A-module. Therefore, since every ideal $\mathfrak{a}$ of B can be viewed as an A-module (remember $A \subseteq B$), $\mathfrak{a}$ is an A-submodule of M and is hence finitely generated; this would show B is Noetherian.

  Since $[K : F]$ is finite, fix a basis $\beta_1, \dots, \beta_m$ for K over F. By Proposition 2.5, we can find a $d \in A$ such that $d\beta_1, \dots, d\beta_m \in B$, and these elements also form a basis for K; therefore to begin with assume the β_i's belong to B. From our discussion after Proposition

1.10, we can also fix a "dual basis" $\beta_1', \dots, \beta_m'$ for K over F such that $\mathrm{Tr}(\beta_i\beta_j') = \delta_{ij}$. We argue that

$$B \subseteq A\beta_1' + A\beta_2' + \cdots + A\beta_m'.$$

For an element $b \in B$, we can write $\beta = b_1\beta_1' + \cdots + b_m\beta_m'$ such that $b_i \in F$. We have to show that in fact $b_i \in A$. Now, by Proposition 2.4, we know that $\mathrm{Tr}(b\beta_i) \in A$, but

$$\mathrm{Tr}(b\beta_i) = \sum_{j=1}^{m} b_j \mathrm{Tr}(\beta_j'\beta_i) = \sum_{j=1}^{m} b_j\delta_{ji} = b_i.$$

This shows B is Noetherian too.

- *Every nonzero prime ideal is maximal:* Suppose $\mathfrak{q}$ is a nonzero prime ideal of B. Then $\mathfrak{p} = \mathfrak{q} \cap A$ has to also be prime. Also, there exists a nonzero $b \in \mathfrak{q}$. By Proposition 2.4 $\mathrm{Nm}(b) \in \mathfrak{q} \cap A = \mathfrak{p}$ and by Proposition 1.10 $\mathrm{Nm}(b) \neq 0$, showing that $\mathfrak{p}$ is nonzero. Since A is a Dedekind domain, $\mathfrak{p}$ must be maximal and so $A/\mathfrak{p}$ is a field. Since $\mathfrak{p} \subseteq \mathfrak{q}$, we can embed $A/\mathfrak{p}$ into the integral domain $B/\mathfrak{q}$ via

  $$a \bmod \mathfrak{p} \mapsto a \bmod \mathfrak{q},$$

  so that $B/\mathfrak{q}$ contains a field over which it is algebraic (since B is integral over A). By Lemma 1.9, $B/\mathfrak{q}$ is therefore a field, and hence $\mathfrak{q}$ is maximal.

□