John Milnor

# Introduction to Algebraic $K$-Theory

# Contents

**Contents** **3**

**1 Projective Modules and $K_0\Lambda$** **5**

1.1 Dedekind Domains . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

# Chapter 1

# Projective Modules and $K_0\Lambda$

The word ring will always mean associative ring with an identity element 1.

Consider left modules over a ring $\Lambda$. Recall that a module $M$ is **free** if there exists a basis $\{m_\alpha\}$ so that each module element can be expressed uniquely as a finite sum $\sum \lambda_\alpha m_\alpha$, and **projective** if there exists a module $N$ so that the direct sum $M \oplus N$ is free. This is equivalent to the requirement that every short exact sequence

$$0 \to X \to Y \to M \to 0$$

must be split exact, so that $Y \cong X \oplus M$.

The **projective module group** $K_0\Lambda$ is an additive group defined by generators and relations as follows. There is to be one generator $[P]$ for each isomorphism class of finitely generated projective modules $P$ over $\Lambda$, and one relation

$$[P] + [Q] = [P \oplus Q]$$

for each pair of finitely generated projectives. (Compare the proof of Lemma 1.1 below.)

Clearly every element of $K_0\Lambda$ can be expressed as the difference $[P_1] - [P_2]$ of two generators. (In fact, adding the same projective module to $P_1$ and $P_2$ if necessary, we may even assume that $P_2$ is free.) We will give a criterion for the equality of two such differences.

First another definition. Let $\Lambda^r$ denote the free module consisting of all $r$-tuples of elements of $\Lambda$. Two modules $M$ and $N$ are called **stably isomorphic** if there exists an integer $r$ so that

$$M \oplus \Lambda^r \cong N \oplus \Lambda^r$$

**Lemma 1.1.** *The generator $[P]$ of $K_0\Lambda$ is equal to the generator $[Q]$ if and only if $P$ is stably isomorphic to $Q$ . Hence the difference $[P_1] - [P_2]$ is equal to $[Q_1] - [Q_2]$ if and only if $P_1 \oplus Q_2$ is stably isomorphic to $P_2 \oplus Q_1$.*

*Proof.* The group $K_0\Lambda$ can be defined more formally as a quotient group $F/R$, where $F$ is free abelian with one generator $\langle P \rangle$ for each isomorphism class of finitely generated projectives $P$, and where $R$ is the subgroup spanned by all $\langle P\rangle + \langle Q\rangle - \langle P \oplus Q\rangle$. (Thus we are reserving the symbol $[P]$ for the residue class of $\langle P\rangle$ modulo $R$.) Note that a sum $\langle P_1\rangle + \cdots + \langle P_k\rangle$ in $F$ is equal to $\langle Q_1\rangle + \cdots + \langle Q_k\rangle$ if and only if

$$P_1 \cong Q_{\pi(1)}, \ldots, P_k \cong Q_{\pi(k)}$$

for some permutation $\pi$ of $\{1, \ldots, k\}$. If this is the case, note the resulting isomorphism

$$P_1 \oplus \cdots \oplus P_k \cong Q_1 \oplus \cdots \oplus Q_k$$

Now suppose that $\langle M\rangle \equiv \langle N\rangle \pmod R$. This means that

$$\begin{aligned}\langle M > - \langle N\rangle = &\sum \left(\langle P_i\rangle + \langle Q_{\mathrm{i}}\rangle - \langle P_i \oplus Q_{\dot{i}}\rangle\right) \\ &- \sum \left(\langle P'_{\mathrm{j}}\rangle + \left\langle Q'_j\right\rangle - \left\langle P'_j \oplus Q'_{j'}\right\rangle\right)\end{aligned}$$

for appropriate modules $P_i, Q_i, P'_j, Q'_j$.

Transposing all negative terms to the opposite side of the equation and then applying the remark above, we get

$$M \oplus \Big(\sum (P_i \oplus Q_i) \oplus \sum P'_j \oplus \sum Q'_j\Big) \cong N \oplus \Big(\sum P_i \oplus \sum Q_i \oplus \sum \left(P'_j \oplus Q'_j\right)\Big),$$

or briefly $M \oplus X \cong N \oplus X$, since the expressions inside the long parentheses are clearly isomorphic. Now choose $Y$ so that $X \oplus Y$ is free, say $X \oplus Y \cong \Lambda^r$. Then adding $Y$ to both sides we obtain $M \oplus \Lambda^r \cong N \oplus \Lambda^r$. Thus M is stably isomorphic to N .

The rest of the proof of Lemma 1.1 is straightforward. □

If the ring $\Lambda$ is commutative, note that the tensor product over $\Lambda$ of (finitely generated projective) left $\Lambda$-modules is again a (finitely generated projective) left $\Lambda$ module. Defining

$$[P] \cdot [Q] = [P \otimes Q]$$

we make the additive group $K_0\Lambda$ into a commutative ring. The identity element of this ring is the class $\left[\Lambda^1\right]$ of the free module on one generator.

In order to compute the group $K_0\Lambda$ it is necessary to ask two questions.

**Question 1.1.** Is every finitely generated projective over $\Lambda$ actually free (or at least stably free)?

**Question 1.2.** Is the number of elements in a basis for a free module actually an invariant of the module? In other words if $\Lambda^r \cong \Lambda^S$ does it follow that $r = s$?

*If both questions have an affirmative answer then clearly $K_0\Lambda$ is the free abelian group generated by $\left[\Lambda^1\right]$. This will be true, for example, if $\Lambda$ is a field, or a skew field, or a principal ideal domain.*

Of course Question 1.1 and Question 1.2 may have negative answers. For example if $\Lambda$ is the ring of endomorphisms of a finite dimensional vector space of dimension greater than 1 , then Chapter 1.1 has a negative answer; and if $\Lambda$ is the ring of endomorphisms of an infinite dimensional vector space then Chapter 1.2 has a negative answer. (The group $K_0\Lambda$ is infinite cyclic but not generated by $[\Lambda^1]$ in the first case, and is zero in the second.)

Here is an important example in which $K_0\Lambda$ is free cyclic.

**Lemma 1.2.** *If $\Lambda$ is a local ring, then every finitely generated*[1] *projective is free, and $K_0\Lambda$ is the free cyclic group generated by $\left[\Lambda^1\right]$.*

*Proof.* First recall the relevant definitions. A ring element $u$ is called a unit if there exists a ring element $v$ with $uv = vu = 1$. The set $\Lambda^\bullet$ consisting of all units in $\Lambda$ evidently forms a multiplicative group.

$\Lambda$ is called a **local ring** if the set $\mathfrak{m} = \Lambda - \Lambda^\bullet$ consisting of all nonunits is a left ideal. It follows that $\mathfrak{m}$ is a right ideal also. For if some product $m\lambda$ with $m \in \mathfrak{m}$ and $\lambda \in \Lambda$ were a unit, then clearly $m$ would have a right inverse, say $mv = 1$. This element $v$ certainly cannot belong to the left ideal $\mathfrak{m}$ . But $v$ cannot be a unit either. For if $v$ were a unit, then the computation

$$m = m\left(v^{-1}\right) = (mv)v^{-1} = v^{-1}$$

would show that $m$ must be a unit.

This contradiction shows that $\mathfrak{m}$ is indeed a two-sided ideal. The quotient ring $\Lambda/\mathfrak{m}$ is evidently a field or skew-field.

Note that a square matrix with entries in $\Lambda$ is non-singular if and only if the corresponding matrix with entries in the quotient $\Lambda/\mathfrak{m}$ is non-singular. To prove this fact, multiply the given matrix on the left by a matrix which represents an inverse modulo $\mathfrak{m}$, and then apply elementary row operations to diagonalize. This shows that the matrix has a left inverse, and a similar argument constructs a right inverse.

We are now ready to prove Chapter 1.2. If the module $P$ is finitely generated and projective over $\Lambda$ then we can choose $Q$ so that $P \oplus Q \cong \Lambda^r$. Thinking of the quotients $P/\mathfrak{m}P$ and $Q/\mathfrak{m}Q$ as vector spaces over the skew-field $\Lambda/\mathfrak{m}$, we can choose bases. Choose a representative in $P$ or in $Q$ for each basis element. The above remark on matrices then implies that the elements so obtained constitute a basis for $P \oplus Q$. Clearly it follows that $P$ and $Q$ are free. Since the dimension of the vector space $P/\mathfrak{m}P$ is an invariant of $P$ , this completes the proof. □

Next consider a homomorphism

$$f : \Lambda \to \Lambda'$$

between two rings. (It is always assumed that $f(1) = 1$.) Then every module $M$ over $\Lambda$ gives rise to a module

$$f_{\#}M = \Lambda' \otimes \Lambda^M$$

[1] Compare [6]

over $\Lambda'$. Clearly if $M$ is finitely generated, or free, or projective, or splits as a direct sum over $\Lambda$, then $f_{\#}M$ is finitely generated, or free, or projective, or splits as as a corresponding direct sum over $\Lambda'$. Hence the correspondence

$$[P] \mapsto [f_{\#}P]$$

gives rise to a homomorphism

$$f_{ast} : K_0\Lambda \to K_0\Lambda'$$

of abelian groups. Note the functorial properties

$$(\text{identity})_{ast} = \text{identity} \qquad (f \circ g)_{ast} = f_{ast} \circ g_{ast}.$$

**Example 1.3.** Let $\boldsymbol{Z}$ be the ring of integers. Then for any ring $\Lambda$ there is a unique homomorphism

$$i : Z \to \Lambda$$

The image

$$i_{ast}\ \mathrm{K}_0 Z \subset K_0\Lambda$$

is clearly the subgroup generated by the free module $[\ \Lambda^1\ ]$. The co-kernel

$$K_0\Lambda/\left(\text{ subgroup generated by }\ [\Lambda^1]\right) = K_0\Lambda/i_{ast}\ \mathrm{K}_0 Z$$

is called the projective class group of $\Lambda$.

**Example 1.4.** Suppose that $\Lambda$ can be mapped homomorphically into a field or skew-field $F$. This is always possible, for example, if $\Lambda$ is commutative. Then we obtain a homomorphism

$$j_{ast} : K_0\Lambda \to K_0\ \mathrm{F} \cong \boldsymbol{Z}$$

In the commutative case, this homomorphism is clearly determined by the kernel of $j$, which is a prime ideal in $\Lambda$. Hence one can speak of the **rank** of a projective module at a prime ideal $\mathfrak{p}$. If $\mathfrak{p} \supset \mathfrak{p}'$, note that the rank at $p$ is equal to the rank at $p'$. For if we localize the integral domain $\Lambda/p'$ at the ideal corresponding to $p$ (that is adjoin the inverses of all elements not belonging to $\mathfrak{p}$) we obtain a local ring which embeds in the quotient field of $\Lambda/p'$ and maps homomorphically into the quotient field of $\Lambda/\mathfrak{p}$. Using Lemma 1.2, it follows that the ranks are equal. *In particular, if $\Lambda$ is an integral domain, then the rank of a projective module is the same at all prime ideals.*

In any case, choosing some fixed homomorphism $j : \Lambda \to F$, since $j_{ast}i_{ast}$ is an isomorphism, we obtain a direct sum decomposition

$$K_0\Lambda = \operatorname{im} i_* \oplus \ker j_*$$

The first summand is free cyclic, and the second maps bijectively to the projective class group of $\Lambda$.

In the commutative case, note that $\ker j_*$ is an ideal in the ring $K_0\Lambda$. We will denote this ideal by $\tilde{K}_0\Lambda$, and write

$$K_0\Lambda \cong \boldsymbol{Z} \oplus \tilde{K}_0\Lambda.$$

**Example 1.5.** Suppose that $\Lambda$ splits as a cartesian product

$$\Lambda_1 \times \Lambda_2 \times \cdots \times \Lambda_k$$

of rings. Then the projection homomorphisms

$$K_0\Lambda \to K_0\Lambda_i$$

give rise to a corresponding cartesian product structure

$$K_0\Lambda \cong K_0\Lambda_1 \times K_0\Lambda_2 \times \ldots \times K_0\Lambda_k$$

The proof is not difficult.

Such a splitting of $\Lambda$ occurs for example whenever $\Lambda$ is commutative and artinian,[2] but is not local. For since $\Lambda$ is commutative, the set of all nilpotent elements forms an ideal. If $\Lambda$ is not local, there must exist an element $\lambda$ which is neither a unit nor a nilpotent element. Since $\Lambda$ is artinian, the sequence of principal ideals

$$(\lambda) \supset \left(\lambda^2\right) \supset \left(\lambda^3\right) \supset \cdots$$

must terminate, say $(\lambda^n) = \left(\lambda^{n+1}\right) = \cdots$ so that $\lambda^n = \rho\lambda^{2n}$ for some $\rho$. But this implies that the element $e = \rho\lambda^n$ is idempotent ( $ee = e$ ), and hence that $\Lambda$ splits as a cartesian product

$$\Lambda \cong \Lambda/(e) \times \Lambda/(1-e)$$

This splitting is not trivial since the hypothesis that $\lambda$ is neither a unit nor nilpotent implies that $e \neq 1, 0$. This procedure can be continued inductively until $\Lambda$ has been expressed as a cartesian product of local rings. It then follows that

$$K_0\Lambda \cong \boldsymbol{Z} \times \boldsymbol{Z} \times \ldots \times \boldsymbol{Z}$$

## 1.1 Dedekind Domains

Important examples in which the ring $K_0\Lambda$ has a more interesting structure are provided by Dedekind domains. We will discuss these in some detail, starting for variety with a non-standard version of the definition. [3]

**Definition 1.** A **Dedekind domain** is a commutative ring without zero divisors such that, for any pair of ideals $\mathfrak{a} \subset \mathfrak{b}$, there exists an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

**Remark 1.1.** Note that the ideal $\mathfrak{c}$ is uniquely determined, except in the trivial case $\mathfrak{a} = \mathfrak{b} = 0$. In fact if $\mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{c}'$, then choosing some nonzero principal ideal $b_0\Lambda \subset \mathfrak{b}$ we can express $b_0\Lambda$ as a product $\mathfrak{x}\mathfrak{b}$ and conclude that $\mathfrak{x}\mathfrak{b}\mathfrak{c} = \mathfrak{x}\mathfrak{b}\mathfrak{c}'$, hence $\mathfrak{b}_0\mathfrak{c} = \mathfrak{b}_0\mathfrak{c}'$, from which the equality $\mathfrak{c} = \mathfrak{c}'$ follows.

[2] A ring is **artinian** if every descrending sequence of ideals must terminate.

[3] The usual definition is of course equivalent to the one given here. For further information, see [10]; or [8]; as well as [3]

**Definition 2.** Two non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in the Dedekind domain $\Lambda$ belong to the same **ideal class** if there exist non-zero ring elements x and y so that $xa = yb$.

Clearly the ideal classes of $\Lambda$ form an abelian group under multiplication, with the class of principal ideals as identity element. We will use the notation $C(\Lambda)$ for the ideal class group of $\Lambda$, and the notation $\{\mathfrak{a}\} \in C(\Lambda)$ for the ideal class of $\mathfrak{a}$.

Note that $\{\mathfrak{a}\} = \{\mathfrak{b}\}$ if and only if $\mathfrak{a}$ is isomorphic, as $\Lambda$-module, to $\mathfrak{b}$. For if $\phi : \mathfrak{a} \to \mathfrak{b}$ is an isomorphism, then choosing $a_0 \in \mathfrak{a}$, the computation $a_0\phi(a) = \phi(a_0 a) = \phi(a_0)\, a$ shows that $a_0\mathfrak{b} = \phi(a_0)\,\mathfrak{a}$.

Important examples of Dedekind domains can be constructed as follows. Let $F$ be a finite extension of the field $\boldsymbol{Q}$ of rational numbers. An element of $F$ is called an **algebraic integer** if it is the root of a monic polynomial

$$x^k + a_1 x^{k-1} + \cdots + a_k$$

with coefficients $a_i \in \boldsymbol{Z}$.

**Theorem 1.2.** *The set $\Lambda = \Lambda(F)$ consisting of all algebraic integers in F is a Dedekind domain, with quotient field $F$.*

The proof of this classical theorem will be deferred until the end of *Chapter* 1.

For such a ring $\Lambda(F)$ of algebraic integers, the ideal class group $C(\Lambda(F)$ ) is always finite. (See for example [9]; or [4]) As examples, for the domains $\boldsymbol{Z}[i], \boldsymbol{Z}[\sqrt{-5}]$, and $\boldsymbol{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$, the ideal class group has order $1, 2$, and $3$ respectively. Further examples will be given in Chapter 3.4.

Projective modules over Dedekind domains can be classified as follows.

**Lemma 1.3.** *Every ideal in a Dedekind domain $\Lambda$ is finitely generated and projective over $\Lambda$. Conversely every finitely generated projective module over $\Lambda$ is isomorphic to a direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_k$ of ideals.*

*Proof.* If $\mathfrak{b}$ is a non-zero ideal, choose $0 \neq a_0 \in \mathfrak{b}$, so $a_0\Lambda \subset \mathfrak{b}$, and define $\mathfrak{c}$ by the equality $a_0\Lambda = \mathfrak{b}c$. Then the generator $a_0$ can be expressed as a finite sum $b_1c_1 + \cdots + b_kc_k$ with $b_i \in \mathfrak{b}, c_i \in \mathfrak{c}$. Define $\Lambda$-linear mappings

$$\mathfrak{b} \to \Lambda^k \text{ and } \Lambda^k \to \mathfrak{b}$$

by the formulas $b \mapsto (bc_1/a_0, \ldots, bc_k/a_0)$ and $(x_1, \ldots, x_k) \mapsto b_1x_1 + \ldots + b_kx_k$. Since the composition is the identity map of $\mathfrak{b}$, this proves that $\mathfrak{b}$ is finitely generated and projective.

Any finitely generated projective $P$ can be embedded in the free module $\Lambda^k$ for some $k$. Projecting to the $k$-th factor we obtain a homomorphism $\phi : P \to \Lambda$ with $\ker\phi \subset \Lambda^{k-1}$.

Since the image $\phi(P) = \mathfrak{a}_k$ is an ideal, hence projective, we have $P \cong \ker\phi \oplus \mathfrak{a}_k$. An easy induction now completes the proof. □

**Remark 1.** More generally, any module which is finitely generated and torsion free over $\Lambda$ can easily be embedded in some $\Lambda^k$ and hence, by this argument, is projective.

**Theorem 1.4** (Steiniz). *Two direct sums $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$ and $\mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ of non-zero ideals are isomorphic as $\Lambda$-modules if and only if $r = s$ and the ideal class $\{\mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_r\}$ is equal to $\{\mathfrak{b}_1\mathfrak{b}_2 \cdots \mathfrak{b}_r\}$*

(Compare [5])

*Proof.* For the first half of the proof, the ring $\Lambda$ can be any integral domain. First note that, if $\mathfrak{a} \subset \Lambda$ is a non-zero ideal, then any $\Lambda$-linear mapping $\phi : \mathfrak{a} \to \mathfrak{b} \subset \Lambda$ determines a unique element $q$ of the quotient field of $\Lambda$ such that

$$\phi(a) = qa \forall a \in \mathfrak{a}$$

To prove this it is only necessary to divide the equation $a_0\phi(a) = \phi\left(a_0 a\right) = \phi\left(a_0\right) a$ by $a_0$, setting $q = \phi\left(a_0\right)/a_0$. Similarly, if the mapping

$$\phi : \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \to \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$$

is $\Lambda$-linear, then there is a unique $s \times r$ matrix $Q = (q_{ij})$ with entries in the quotient field so that the $i$-th component of $\phi\left(a_1, \ldots, a_r\right) = (b_1, \ldots, b_S)$ is

$$b_i = \sum q_{ij} a_j$$

for all $(a_1, \ldots, a_r) \in \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$. If $\phi$ is an isomorphism, then this matrix $Q$ has an inverse, hence $r = s$. We then assert that the product ideal $\mathfrak{b}_1 \cdots \mathfrak{b}_r$ is equal to $\det(Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r$. In fact for each generator $a_1 \ldots a_r$ of $a_1 \ldots a_r$, the product $\det(Q) a_1 \ldots a_r$ can be expressed as the determinant of the product matrix

$$Q\left(\begin{bmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & a_r \end{bmatrix}\right).$$

whose $i$-th row consists completely of elements $q_{ij}a_j$ of $\mathfrak{b}_i$. This proves that

$$\det(Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r \subset \mathfrak{b}_1 \cdots \mathfrak{b}_i$$

A similar argument shows that

$$\det(Q^{-1}\mathfrak{b}_1 \cdots \mathfrak{b}_r \subset \mathfrak{a}_1 \cdots \mathfrak{a}_r$$

Multiplying this last inclusion by $\det(Q)$ and comparing, it follows that $\mathfrak{b}_1 \cdots \mathfrak{b}_r$ is equal to $\det(Q)\mathfrak{a}_1 \cdots \mathfrak{a}_r$; and hence belongs to the ideal class $\{a_1 \cdots a_r\}$. This proves the first half of Theorem 1.4.

To prove that the rank $r$ and the ideal class $\{\mathfrak{a}_1 \cdots \mathfrak{a}_r\}$ form a complete invariant for $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r$, it clearly suffices to prove the following.

**Lemma 1.5.** *If $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals in a Dedekind domain $\Lambda$, then the module $\mathfrak{a} \oplus \mathfrak{b}$ is isomorphic to $\Lambda^1 \oplus (\mathfrak{a}\mathfrak{b})$.*

*Proof.* If $\mathfrak{a}$ and $\mathfrak{b}$ happen to be relatively prime ($\mathfrak{a} + \mathfrak{b} = \Lambda$), the proof proceeds as follows. Map $\mathfrak{a} \oplus \mathfrak{b}$ onto $\Lambda^1$ by the correspondence $\mathfrak{a} \oplus \mathfrak{b} \mapsto \mathfrak{a} + \mathfrak{b}$. The kernel is clearly isomorphic to the module $\mathfrak{a} \cap \mathfrak{b}$. Since $\Lambda^1$ is projective, the sequence $0 \to \mathfrak{a} \cap \mathfrak{b} \to \mathfrak{a} \oplus \mathfrak{b} \to \Lambda^1 \to 0$ is split exact, and therefore $\mathfrak{a} \oplus \mathfrak{b} \cong \Lambda^1 \oplus (\mathfrak{a} \cap \mathfrak{b})$. But the intersection $\mathfrak{a} \cap \mathfrak{b}$ is equal to the product ideal $\mathfrak{a}\mathfrak{b}$. For the inclusion $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ is clear; and if $1 = a_0 + b_0$ then every $x \in \mathfrak{a} \cap \mathfrak{b}$ can be expressed as $x = a_0 x + x b_0$, and hence belongs to $\mathfrak{a}\mathfrak{b}$. Thus $\mathfrak{a} \oplus \mathfrak{b} \cong \Lambda^1 \oplus \mathfrak{a}\mathfrak{b}$ as required.

For the general case, the hypothesis that $\Lambda$ is a Dedekind domain will be needed in order to replace $\mathfrak{a}$ by an ideal which is relatively prime to $\mathfrak{b}$. It clearly suffices to prove the following.

**Lemma 1.6.** *Given non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a Dedekind domain $\Lambda$ there exists an ideal $\mathfrak{a}'$ in the ideal class of $\mathfrak{a}$ which is prime to $\mathfrak{b}$.*

To prove this we must first establish two of the standard properties of Dedekind domains.

**Lemma 1.7.** *Every non-zero ideal in a Dedekind domain $\Lambda$ can be expressed uniquely as a product of maximal ideals.*

*Proof.* In fact choosing any maximal ideal $\mathfrak{m}_1 \supset \mathfrak{a}$ we have $\mathfrak{a} = \mathfrak{m}_1\mathfrak{a}_1$ for some ideal $\mathfrak{a}_1$, then similarly $\mathfrak{a}_1 = \mathfrak{m}_2\mathfrak{a}_2$, and so on, with $\mathfrak{a} \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ This sequence must terminate, since $\Lambda$ is Noetherian by Lemma 1.3. The resulting factorization is unique. For if $\mathfrak{m}_1 \cdots \mathfrak{m}_k = \mathfrak{m}'_1 \cdots \mathfrak{m}'_\ell$ then $\mathfrak{m}'_1 \supset \mathfrak{m}_1 \cdots \mathfrak{m}_k$ and hence, since $\mathfrak{m}'_1$ is prime, $\mathfrak{m}'_1$ contains some $\mathfrak{m}_i$, and therefore is equal to $m_i$. The uniqueness statement then follows by induction on $\mathrm{Max}(k, \ell)$, using Remark 1.1. □

**Lemma 1.8.** *For any non-zero ideal $\mathfrak{a}$ in a Dedekind domain $\Lambda$, the quotient $\Lambda/\mathfrak{a}$ is a principal ideal ring (usually with zero divisors).*

*Proof.* Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ be the distinct maximal ideals containing $\mathfrak{a}$. We will first show that each $\mathfrak{m}_i$ is a principal ideal modulo $\mathfrak{a}$. Let $x_1$ be a ring element which belongs to $\mathfrak{m}_1$ but not to $\mathfrak{m}_1^2$. Since the ideals $\mathfrak{m}_1^2, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ are pairwise relatively prime (using Lemma 1.7), it follows that there exists a ring element $y_1$ so that

$$\begin{aligned} y_1 &\equiv x_1 \pmod{\mathfrak{m}_1^2} \\ y_1 &\equiv 1 \pmod{\mathfrak{m}_j} \text{ for } j > 1 \end{aligned}$$

using the Chinese Remainder Theorem. (See for example [7]) Then the ideal generated by $y_1$ and $\mathfrak{a}$ is contained in $\mathfrak{m}_1$, but is not contained in $\mathfrak{m}_1^2$ or in any other maximal ideal. So, using Lemma 1.7, this ideal can only be $\mathfrak{m}_1$ itself.

This proves that $\mathfrak{m}_1$ is a principal ideal modulo $\mathfrak{a}$. But every ideal of $\Lambda/a$ is a product of maximal ideals, so this completes the proof of Lemma 1.8. □

We are now ready to prove Lemma 1.6. Given non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$, choose $0 \neq a_0 \in \mathfrak{a}$ and define $\mathfrak{x}$ by the equation $\mathfrak{x}\mathfrak{a} = a_0\Lambda$. Applying Lemma 1.8 to the ideal $\mathfrak{x}$ modulo $\mathfrak{b}x$, we see that $\mathfrak{x}$ is generated by $\mathfrak{b}x$ together with some element $x_0$. Now multiplying the equation

$$\mathfrak{x} = \mathfrak{b}\mathfrak{x} + \mathfrak{x}_0\Lambda$$

by $\mathfrak{a}$, and then dividing by $a_0$, we obtain

$$\Lambda = \mathfrak{b} + \mathfrak{a}x_0/a_0$$

Since $\mathfrak{a}x_0/a_0$ is clearly an ideal in the ideal class $\{\mathfrak{a}\}$, this proves Lemma 1.6. □

Hence this completes the proof of Theorem 1.4. □

**Corollary 1.9.** *If $\Lambda$ is a Dedekind domain, then $K_0\Lambda \cong \boldsymbol{Z} \oplus \tilde{K}_0\Lambda$, where the additive group of $\tilde{K}_0\Lambda$ is canonically isomorphic to the ideal class group $C(\Lambda)$, and where the product of any two elements in the ideal $\tilde{K}_0\Lambda$ is zero.*

*Proof.* In fact the correspondence

$$[\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r] \mapsto (r, \{\mathfrak{a}_1 \cdots \mathfrak{a}_r\})$$

maps $K_0\Lambda$ isomorphically onto $\boldsymbol{Z} \oplus C(\Lambda)$. Recall that $\tilde{K}_0\Lambda$ can be identified with the set of differences $[P] - [Q]$ with $\operatorname{rank} P = \operatorname{rank} Q$. Then each element of $\tilde{K}_0\Lambda$ can be written as a difference $[\mathfrak{a}] - \left[\Lambda^1\right]$, and we must prove that

$$\left([\mathfrak{a}] - \left[\Lambda^1\right]\right)\left([\mathfrak{b}] - \left[\Lambda^1\right]\right) = 0$$

But the product $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a} \otimes \mathfrak{b}]$ is equal to $[\mathfrak{a}\mathfrak{b}]$. In fact the projective modules $\mathfrak{a} \otimes \mathfrak{b}$ and $\mathfrak{a}\mathfrak{b}$ both have rank 1, so the natural surjection from the tensor product to the product ideal is an isomorphism. The conclusion now follows from **??**. □

**Remark 2.** The ideal class group $C(\Lambda)$ can be naturally identified with a multiplicative group, $1 + \tilde{K}_0\Lambda$, of units in the ring $K_0\Lambda$. Something similar happens for an arbitrary commutative ring. Call a module M , over a commutative ring $\Lambda$, **invertible** if there exists a module $N$ so that $M \otimes N$ is free on one generator. The set of isomorphism classes of invertible modules clearly forms a group under the tensor product. This group is called the **Picard group**, denoted by $\mathrm{Pic}(\Lambda)$.

It can be shown that a module is invertible if and only if is projective, finitely generated, and has rank 1 at every prime ideal. (Compare [1]) Furthermore the second exterior power $E^2_\Lambda M$ of an invertible module is zero. For this exterior power is a projective module which has rank zero at every prime. ([2]) It follows that the Picard group embeds as a subgroup of the group of units in $K_0\Lambda$. For if two invertible modules $M$ and $M'$ are stably isomorphic, $M \oplus \Lambda^r \cong M' \oplus \Lambda^r$, then taking the $(r+1)$-st exterior power of each side, we see that $M \cong M'$. (Bass proves the sharper statement that there exists a canonical retracting homomorphism from the additive group of $K_0\Lambda$ to the multiplicative group $\mathrm{Pic}(\Lambda) \subset K_0\Lambda$.)

In the case of a Dedekind domain, it is clear that $\mathrm{Pic}(\Lambda)$ is canonically isomorphic to the ideal class group $C(\Lambda)$.

To conclude Chapter 1, let us prove Theorem 1.2. If $F$ is a finite extension of the field of rational numbers, we must show that the set $\Lambda$, consisting of all algebraic integers in $F$, is a Dedekind domain.

Let $n$ be the degree of $F$ over $\boldsymbol{Q}$ . It will be convenient to use the word lattice to mean an additive subgroup of $F$ which has a finite basis. Thus every lattice $L$ in $F$ is a free abelian additive group of rank $\leq n$. The product $LL'$ of two lattices in $F$ is the lattice generated by all products $\ell\ell'$ with $\ell \in L$ and $\ell' \in L'$.

**Lemma 1.10.** *An element $f$ of $F$ is an algebraic integer if and only if there exists a non-zero lattice $L \subset F$ with $fL \subset L$.*

*Proof.* For if $f$ is a root of the polynomial $x^k+a_1x^{k-1}+\cdots+a_k$ with coefficients in $\boldsymbol{Z}$, then the field elements $1, f, f^2, \ldots f^{k-1}$ span a lattice $L = \boldsymbol{Z}[f]$ with $fL \subset L$. Conversely, if $fL \subset L$ where $L$ is spanned by $b_1, \ldots, b_k$, then we can set

$$fb_i = \sum_j a_{ij} b_j$$

for some matrix $(a_{ij})$ of rational integers. Writing this as

$$\sum_j \left(f\delta_{ij} - a_{ij}\right) b_j = 0,$$

where $(\delta_{ij})$ denotes the $k \times k$ identity matrix, it follows that the columns of the matrix $(f\delta_{ij} - a_{ij})$ are linearly dependent. Therefore $f$ satisfies the monic polynomial equation

$$\det\left(f\delta_{ij} - a_{ij}\right) = 0$$

with coefficients in $\boldsymbol{Z}$; which proves Lemma 1.10. □

It follows that the set $\Lambda$, consisting of all algebraic integers in F , is closed under addition and multiplication. For if $\lambda, \mu \in \Lambda$, then there exist lattices $L$ and $L'$ with

$$\lambda L \subset L, \quad \mu L' \subset L'$$

Now the product lattice $L'' = L'$ will satisfy $(\lambda+\mu)L'' \subset L''$ and $\lambda\mu L'' \subset L''$. Thus $\Lambda$ is a ring.

**Lemma 1.11.** *This set $\Lambda \subset F$ is itself a lattice of rank $n$ in $F$.*

*Proof.* The proof will be based on the trace homomorphism from $F$ to $\boldsymbol{Q}$. If $F' \supset F$ is a Galois extension of $\boldsymbol{Q}$ , recall that the additive homomorphism

$$\mathrm{tr}_{F/\boldsymbol{Q}} : F \to \boldsymbol{Q}$$

can be defined by the formula

$$\mathrm{tr}_{F/\boldsymbol{Q}}(f) = \sigma_1(f) + \cdots + \sigma_n(f),$$

where $\sigma_1, \ldots, \sigma_n$ are the distinct embeddings of $F$ in $F'$. (See, for example, [7])

Note that the set of algebraic integers in $\boldsymbol{Q}$ is precisely equal to $\boldsymbol{Z}$. For if a fraction $\frac{a}{b}$ satisfies a monic polynomial equation with coefficients in $\boldsymbol{Z}$, then clearing denominators we see that every prime which divides $b$ must also divide $a$.

Therefore the trace homomorphism from $F$ to $\boldsymbol{Q}$ maps $\Lambda$ into $\boldsymbol{Z}$. For if $\lambda \in \Lambda$, then trace $F/\boldsymbol{Q}(\lambda)$ is both an algebraic integer (in $F'$) and a rational number; hence $\mathrm{tr}_{F/\boldsymbol{Q}}(\lambda) \in \boldsymbol{Z}$.

Note that every field element $f$ possesses a multiple $f + f + \cdots + f = mf$ which is an algebraic integer. In fact, expressing $f$ as the root of a polynomial with integer coefficients, we can take $m$ to be the absolute value of the leading coefficient. It follows that the quotient field of $\Lambda$ is equal to $F$.

Consider the $\boldsymbol{Q}$-bilinear pairing

$$f, f' \mapsto \mathrm{tr}_{F/\boldsymbol{Q}}\left(ff'\right)$$

from $F \times F$ to $\boldsymbol{Q}$. This pairing is non-degenerate, since for each $f \neq 0$ we can choose $f' = 1/f$ so that $\mathrm{tr}(ff') \neq 0$. Choose algebraic integers $\lambda_1, \ldots, \lambda_n$ which form a basis for $F$ over $\boldsymbol{Q}$ . Then the $\boldsymbol{Q}$-linear function

$$f \mapsto \left(\mathrm{tr}_{F/\boldsymbol{Q}}\left(\lambda_1 f\right), \ldots, \mathrm{tr}_{F/\boldsymbol{Q}}\left(\lambda_n f\right)\right)$$

from $F$ to $\boldsymbol{Q} \oplus \cdots \oplus \boldsymbol{Q}$ is bijective, and embeds $\Lambda$ in the direct sum $\boldsymbol{Z} \oplus \cdots \oplus \boldsymbol{Z}$. Therefore $\Lambda$ is finitely generated as additive group; which proves Lemma 1.11. □

It follows that every non-zero ideal $\mathfrak{a} \subset \Lambda$ is also a lattice of rank $n$ in $F$. Here are three important consequences of Lemma 1.11.

1. *The ring* $\Lambda$ *is Noetherian.*
   In fact, if $\mathfrak{a}$ is a non-zero ideal, then $\Lambda/\mathfrak{a}$ is finite, so there are only finitely many larger ideals.

2. *Every non-zero prime ideal of* $\Lambda$ *is maximal.*
   For the quotient ring $\Lambda/\mathfrak{p}$, being finite and without zero divisors, must be a field.

3. *If an element* $f$ *in the quotient field of* $\Lambda$ *satisfies* $f\mathfrak{a} \subset \mathfrak{a}$ *for some non-zero ideal* $\mathfrak{a}$*, then* $f \in \Lambda$*.*
   In other words $\Lambda$ is integrally closed in its quotient field. This follows using Lemma 1.10.

We will show that any domain satisfying (1), (2) and (3) is necessarily Dedekind. The proof, due to van der Waerden, is based on the following.

**Observation 3.** Every non-zero ideal a in a commutative Noetherian ring contains a product of non-zero prime ideals.

For if $\mathfrak{a}$ itself is prime, there is nothing to prove. Otherwise, choosing ring elements $\lambda$ and $\mu$ not in $\mathfrak{a}$ so that $\lambda\mu \in \mathfrak{a}$, the two ideals $\mathfrak{a} + \lambda\Lambda$ and $\mathfrak{a} + \mu\Lambda$ are strictly larger than $\mathfrak{a}$, but have product contained in $\mathfrak{a}$. Assuming inductively that the Observation is true for these two larger ideals, it follows that it is true for $\mathfrak{a}$ also. (This "induction" argument makes sense since $\Lambda$ is Noetherian.)

Now given a domain $\Lambda$ satisfying (1), (2) and (3), and given non-zero ideals $\mathfrak{a} \subset \mathfrak{b}$, we must show that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ for some ideal $\mathfrak{c}$. We will assume inductively that this statement is true for any ideal $\mathfrak{b}'$ which is strictly larger than $\mathfrak{b}$; and for any $\mathfrak{a}' \subset \mathfrak{b}'$. To start the induction, the statement is certainly true when $\mathfrak{b} = \Lambda$.

Choose an element $b \neq 0$ in $\mathfrak{b}$, and choose a product $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ of maximal ideals so that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \Lambda b$, with $r$ minimal. Also choose a maximal ideal $\mathfrak{p} \supset \mathfrak{b}$. Then $\mathfrak{p}$ contains the product $\mathfrak{p}_1 \cdots \mathfrak{p}_{\mathfrak{r}}$, hence $\mathfrak{p}$ contains some $\mathfrak{p}_i$, and therefore $\mathfrak{p} = \mathfrak{p}_i$. To fix our ideas, assume that $\mathfrak{p} = \mathfrak{p}_1$. The product $\mathfrak{p}_2 \cdots \mathfrak{p}_r$ is not contained in $\Lambda b$, since $r$ is minimal, so there exists an element $c \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ with $c \notin \Lambda b$. Evidently

$$c\mathfrak{b} \subset c\mathfrak{p} \subset \mathfrak{p}_2 \cdots \mathfrak{p}_r \mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \Lambda b$$

Therefore

$$(c/b)\mathfrak{b} \subset \Lambda$$

even though the element $c/b \in F$ does not belong to $\Lambda$. Consider the ideal

$$\mathfrak{b}' = b^{-1}(\Lambda b + \Lambda c)\mathfrak{b} = \mathfrak{b} + (c/b)\mathfrak{b}$$

in $\Lambda$. Since $c/b \notin \Lambda$, it follows from (3) that $\mathfrak{b}'$ is strictly larger than $\mathfrak{b}$. Therefore, by the induction hypothesis, given any $\mathfrak{a} \subset \mathfrak{b}$ the equation

$$\mathfrak{a} = \mathfrak{b}'\mathfrak{c}'$$

has a solution c'. Setting

$$c = b^{-1}(\Lambda b + \Lambda c)\mathfrak{b}\mathfrak{c}' \subset F$$

we have

$$\mathfrak{b}\mathfrak{c} = b^{-1}(\Lambda\mathfrak{b} + \Lambda\mathfrak{c})\mathfrak{b}\mathfrak{c}' = \mathfrak{b}'\mathfrak{c}' = \mathfrak{a},$$

are required. This set $\mathfrak{c}$ is actually contained in $\Lambda$, since it satisfies the condition $\mathfrak{b}\mathfrak{c} \subset \mathfrak{b}$. (Compare (3).) This shows that $\Lambda$ is a Dedekind domain, and completes the proof of Theorem 1.2.