Notes for Seminar in Algerbaic K-Theory

Texed by Lin-Da Xiao

October 9, 2017

Contents

1 September 25th

Convention: A ring always means an associative ring with unit, (not necessarily commutative).

Definition 1.1. *Consider a module M over a ring Λ, it is called **free** if there exists a basis $\{m_\alpha\}$, and **projective** if there is a module N s.t. $M \oplus N$ is free.*

Proposition 1.2. *A module M is projective iff the exact sequence $0 \to E \to F \to M \to 0$ splits.*

Proof. ¿¿¿¿¿¿ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Definition 1.3. *The projective module group $K_0\Lambda$ is an additive group generated by generators $[P]$, there is one generator $[P]$ corresponding to the isomorphism classes of finitely generated projective module P (the correspondence is not one to one). And it has one relation*

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

General elements in $K_0\Lambda$ is the formal difference $[P] - [Q]$. Clearly, it is a group:
$$[0] + [P] = [P \oplus 0] \implies [0] \text{ is the identity element}$$

$$[P] + (-[P]) = [0].$$

Definition 1.4. *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 1.5. *The generator $[P]$ of $K_0\Lambda$ is equal to the generator $[Q]$ iff P is stably isomorphic to Q. Hence the difference $[P_1] - [P2]$ is equal to $[Q_1] - [Q_2]$ iff $P_1 \oplus Q_1$ is stably isomorphic to $P_2 \oplus Q_1$.*

Proof. The group $K_0\Lambda$ can be identified as a quotient group F/R, where F is the free Abelian group generated with the $\langle P \rangle$ of for each isomorphism class of finitely generated projective module P, and where R is the sub group spanned by all $\langle P \rangle + \langle Q \rangle - \langle P \oplus Q \rangle$. (We reserve the symbol $[P]$ for the residue class of $\langle P \rangle \mod R$).

Note that in the free Abelian group two sums $\sum_i^n \langle P_i \rangle$ and $\sum_j^m Q_j$ are equal iff
$$n = m,$$
and
$$\{P_1, ..., P_n\} = \{Q_1, ..., Q_n\}.$$
Then
$$\langle M \rangle - \langle N \rangle = \sum_i \langle P_i \rangle + \langle Q_i \rangle - \langle P_i \oplus Q_i \rangle$$
$$- \sum_j \left(\langle P_j' \rangle + \langle Q_j' \rangle - \langle P_j' \oplus Q_j' \rangle \right)$$
then we have
$$\langle M \rangle + \sum_i \langle P_i \oplus Q_i \rangle + \sum_j (\langle P_j' \rangle + \langle Q_j' \rangle) = \langle N \rangle + \sum_i \langle P_i' \oplus Q_i' \rangle + \sum_j (\langle P_j \rangle + \langle Q_j \rangle)$$
$$\implies M \oplus \left(\sum_i (P_i \oplus Q_i) \oplus \sum_j P_j' \oplus \sum_j Q_j' \right) = N \oplus \left(\sum_i P_i \oplus \sum_i Q_i \oplus \sum_j (P_j' \oplus Q_j') \right)$$
and then
$$M \oplus X = N \oplus X.$$
X is a finite direct sum of projective modules, thus still projective. We can choose Y such that $X \oplus Y = \Lambda^s$. Then we get
$$M \oplus \Lambda^s = N \oplus \Lambda^s.$$

Then converse direction is just trivial . $\qquad\square$

Together with the tensor-product, $[P] \cdot [Q] = [P \otimes Q]$. The multiplication is distributive over the addition and we make $K_0 \lambda$ into a commutative ring, where the identity element is the class $[\Lambda^1]$.

In order to calculate the the group $K_0 \Lambda$, it is necessary to ask two questions:

- Is every finitely generated projective over Λ actually free or stably free?

- Is it true that $\Lambda^s \cong \Lambda^t$ iff $s = t$?

If both questions have an affirmative answer, then $K_0\Lambda$ is a boring free Abelian group generated by $[\Lambda^1]$, which is true when Λ is a field , skew field and PID. (All module over field or division ring is free, all projective modules over PID are free) And the second question is true for nontrivial commutative rings with unit.

Example 1.6. *For $\Lambda = \mathbb{Z}$,*

$$K_0\mathbb{Z} = \mathbb{Z}.$$

Proof. Λ is a PID and we know that every finitely generated projective is free over a PID (Free module are of the form Λ^s). $\mathbb{Z}$-modules are just Abelian groups, by the classification of finitely generated Abelian group, we have

$$M \cong \Lambda^r \oplus (\oplus_i \Lambda/(p_i^{\alpha_i}))$$

for $r \geq 0$,p_i prime number, and $\alpha_i \geq 0$. M projective, i.e. $\exists N : M \oplus N \cong \Lambda^s$. Then, N also is finitely generated,

$$\begin{aligned}
&\implies \Lambda^s = \Lambda^r \oplus_i \oplus \Lambda/(p_i^{\alpha_i}) \oplus \Lambda^t \oplus_j \oplus \Lambda/(q_j^{\beta_j}) \\
&\implies \Lambda^s \cong \Lambda^r \oplus \Lambda^t \\
&\implies M = \Lambda^r \text{ and } N = \Lambda^t \\
&\implies K_0\Lambda = \mathbb{Z}
\end{aligned}$$

$\square$

Lemma 1.7. *If Λ is a local ring, then every finitely generated projective is free, and $K_0\Lambda$ is the free Abelian cyclic group generated by $[\Lambda^1]$*

Proof.

- Recall that a ring is local if it has a unique maximal left ideal $\mathfrak{m}$. This left ideal is automatically a maximal right ideal. The unique maximal ideal consists of all the non-units in the ring, each element $m \in \mathfrak{m}$ and right multiply it with an element $\lambda \in \Lambda$, $m\lambda$ can not be a unit. Otherwise, $\exists v \in \Lambda$ s.t. $mv = 1 \implies m = v^{-1}$. Then we get the contradiction that m is a unit. Hence, $\mathfrak{m}$ is a two sided ideal, and $\Lambda/\mathfrak{m}$ is a field or skew field. (Division rings or skew-fields differ form a field only in that their multiplication is not necessarily commutative)[1]

---

[1]However, by Wedderburn's little theorem all finite division rings are commutative and therefore finite fields.

4

- Note that a square matrix with entries in Λ is invertible iff the corresponding matrix with entries in the quotient $\Lambda/\mathfrak{m}$ is invertible. To prove this fact, multiply the given matrix on the left by a matrix which represents an inverse modulo $\mathfrak{m}$, and the apply elementary row operations to diagonalize, we will see in the end, the product is identity matrix modulo $\mathfrak{m}$. This shows that the matrix has a left inverse, the right inverse is similar.

- If the module P is finitely generated and projective over Λ then we can choose Q so that $P \oplus Q \cong \Lambda^r$. Think 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 of $P \oplus Q$. Clearly it follows that P and Q are free. The number of elements in a basis for the free module is actually an invariant of the module because the dimension of $P/\mathfrak{m}P$ is indeed an invariant of the module.

$\square$

Now consider a ring homomorphism $f : \Lambda \to \Lambda'$. Then it induces a morphism of Λ-modules

$$f_\# : M \to \Lambda' \otimes_\Lambda M,$$

the later is in fact a Λ'-module. Clearly if M is finitely generated, or free, or projective, or splits as a direct sum over Λ, $f_\# M$ is respectively finitely generated, or free, or projective, or splits as a direct sum over Λ'. Hence the correspondence

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

gives rise to a homomorphism

$$f_* : K_0\Lambda \to K_0\Lambda$$

of Abelian groups, i.e. K_0 is a functor from {Associative Rings} to {Abelian groups}.

Example 1.8. *Consider $I : \mathbb{Z} \to \Lambda$, $k \mapsto k\mathbb{1}_\Lambda$, we claim $G := I_*(K_0\mathbb{Z})$ is a cyclic group*

Proof. $I(\mathbb{Z})$ is a subring of Λ, by the functorial properties, we know $G = I_*(K_0\mathbb{Z})$ is the subgroup generated by the free module $[\Lambda^1]$, which is obviously cyclic. $\qquad\square$

$K_0\Lambda/G$ is called the **projective class group** .

Example 1.9. *Consider ring morphism $J : \Lambda \to \mathbb{F}$, $\mathbb{F}$ is a (skew) field, which is always possible for commutative rings. We already know that $K_0\mathbb{F} \cong \mathbb{Z}$. Then we claim that J_*I_* is an isomorphism and $K_0\Lambda = Im(I_*) \oplus Ker(J_*)$. The first summand is free cyclic and the second is isomorphic to the projective class group of Λ.*

Proof.
I_* is injective;
Because the $I_*([P]) = 0 \implies [I_\#(P)] = [\Lambda \otimes_\mathbb{Z} P] = 0 \implies (\Lambda \otimes_\mathbb{Z} P) \oplus \Lambda^t \cong \Lambda^s$,
thus $\Lambda \otimes_\mathbb{Z} P$ is stably free. ????????? possibly means P is stably free?
J_* is surjective;
All modules over field or skew field are free, then in general we have, W is a finitely generated $\mathbb{F}$-module, then $[W] \in K_0\mathbb{F} \implies W = \mathbb{F}^s = [\mathbb{F} \otimes_\Lambda \Lambda^s] = J_*([\Lambda^s])$.

$$0 \longrightarrow K_0\mathbb{Z} \xrightarrow{I_*} K_0\Lambda \xrightarrow{J_*} K_0\mathbb{F} \longrightarrow 0$$

Notice that the sequence is not an exact sequence. But we know I_* is injective, J_* is surjective and also $K_0\mathbb{Z} = K_0\mathbb{F} = \mathbb{Z}$, then we can conclude that J_*I_* is an isomorphism. And then $K_0\Lambda \cong Im(I_*) \oplus Ker(J_*)$ $\qquad\square$

Remember $Im(I_*)$ is free cyclic if Λ is commutative. $Im(I_*) \cong \mathbb{Z}$. Then we have

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

$ker(J_*)$ maps bijectively to the projective class group $K_0\Lambda/\langle\Lambda\rangle$, where we denote $\tilde{K}_0\Lambda$ for commutative case.

Example 1.10.
$$\Lambda = \Lambda_1 \times ... \times \Lambda_k$$

$$\implies K_0\Lambda \cong K_0\Lambda_1 \times ... \times K_0\Lambda_k$$

Proof. Theorem(6.6) in *[Magurn] An Algebraic Introduction to K-Theory.* $\qquad\square$

Application: We assume Λ is Artinian[2] commutative but not local.

1. $\mathfrak{m} = \{\lambda \in \Lambda | \exists k \geq 0; \lambda^k = 0\}$ is an ideal.

2. Λ is not local $\implies \exists \hat{\lambda} \in \Lambda \backslash (\Lambda^\times \cup \mathfrak{m})$

suppose $\forall \lambda \in \Lambda; \lambda \in \Lambda^\times$ or $\lambda \in \mathfrak{m}$. Then $\Lambda \backslash \Lambda^\times = \mathfrak{m}$ is an ideal $\implies \Lambda$ local.

3. Since Λ is Artinian, the sequence of principal ideals

$$(\hat{\lambda}) \supset (\hat{\lambda}^2) \supset (\hat{\lambda}^3) \supset \dots$$

must terminate. Suppose $(\hat{\lambda}^n) = (\hat{\lambda}^{n+1})$, so that $\hat{\lambda}^n = \rho \hat{\lambda}^{2n}$ for some ρ. But this implies that $e = \rho \hat{\lambda}^n$ is idempotent and hence Λ splits as a Cartesian product

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

The splitting is nontrivial because e is not 0 or 1. This procedure can continue until Λ has been expressed as Cartesian product of local rings. It follows that

$$K_0 \Lambda \cong \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}.$$

Some Number Theory and Dedekind Domains

————————————-personal notes

Definition 1.11. *Suppose $\mathcal{R}$ is a commutative integral domain. An elemnet of $\mathcal{R}$ is **composite** if it is a product of two nonzero nonunits of $\mathcal{R}$. An element of $\mathcal{R}$ is **irresducible** if it is not zero , not a unit, and not a composite. We say $\mathcal{R}$ is **factorial** with respect to T if $T \subset R - \{0\}$ and each $r \in \mathcal{R} - \{0\}$ can be uniquely written inthe form*

$$r = u \prod_{p \in T} p^{n(p)},$$

where u is unit and $n(p)$ are nonnegative integers that are zero for all but finitely manuy $p \in T$.

By the uniqueness, we know that each element of T is nonunit. Then we know, r is

- unit, iff $\sum n(p) = 0$

- composite, iff $\sum n(p) > 1$

---

[2]Artinian means every descending sequence of ideals must terminate

- irreducible, iff $\sum n(p) = 1$

The set T is not uniquely determined by the factorial ring $\mathcal{R}$: If $\mathbb{F}$ is the field of fractions of $\mathcal{R}$, then $\mathcal{R}^\times$ is a (normal) subgroup of $\mathbb{F}^\times$. The set of irreducibles in $\mathcal{R}$ is a union of some of the cosets of $\mathcal{R}^*$. The factorial ring $\mathcal{R}$ is factorial with respect to T if and only if T consists of exactly one representative from each coset of irreducibles from $\mathcal{R}$.

Definition 1.12. $\mathfrak{a}$ *and* $\mathfrak{b}$ *are ideals in a commutative ring* $\mathcal{R}$, *we write* $\mathfrak{a}|\mathfrak{b}$ *if* $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ *for an ideal* $\mathfrak{c}$.

Theorem 1.13. *For elements* α *and* β *in* $\mathcal{R}$, $\alpha|\beta$ *iff* $(\alpha)|(\beta)$.

Proof. If $\alpha\gamma = \beta$, for principal ideals we have $(\alpha)(\gamma) = (\alpha\gamma) = (\beta)$. Conversely for $(\alpha)|(\beta)$, we have $(\beta) = (\alpha)\mathfrak{c} = \alpha\mathfrak{c}$, then $\beta \in \alpha\mathfrak{c}$, the we get the conclusion. $\qquad\square$

——————————-

Definition 1.14. *A* **Dedekind domain** *is an integral domain s.t. for any pair of ideals* $\mathfrak{a} \subset \mathfrak{b}$, *there exists an ideal* $\mathfrak{c}$ *with* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Remark 1.15. *The ideal* $\mathfrak{c}$ *is uniquely determined, except in the trivial case* $\mathfrak{a} = \mathfrak{b} = 0$. *If* $\mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{c}'$, *then we can consider the principal ideal* $(b_0) \subset \mathfrak{b}$. *By the associativity of ideal multiplication, we have* $(b_0)\mathfrak{b}\mathfrak{c} = (b_0)\mathfrak{b}\mathfrak{c}' \implies (b_0)\mathfrak{c} = (b_0)\mathfrak{c}' \implies b_0\mathfrak{c} = b_0\mathfrak{c}'$, *from which we conclude that* $\mathfrak{c} = \mathfrak{c}'$, *because there is no zero divisors.*

Definition 1.16. *Let* $\mathfrak{a} \neq 0 \neq \mathfrak{b}$ *be two ideals in a Dedekind domain* Λ. *They belong to the same ideals class if* $\exists x, y \in \Lambda\backslash 0$ *s.t.* $x\mathfrak{a} = y\mathfrak{b}$. *We use* $\{\mathfrak{a}\}$ *to denote the ideal class of* $\mathfrak{a}$.

Proposition 1.17.

- $\{\mathfrak{a}\} = \{\mathfrak{b}\} \iff \mathfrak{a} \cong \mathfrak{b}$ *as* Λ *modules.*

- *The ideal classes form multiplicative group with the class of principal ideals as identity element. We will use the notation* $C(\Lambda)$ *for the ideal class group of* Λ.

Proof. For the first statement, we check that if $\phi : \mathfrak{a} \to \mathfrak{b}$ is an isomorphism of Λ-modules, then choosing $a_0 \in \mathfrak{a}$, the computation $a_0\phi(\mathfrak{a}) = \phi(a_0\mathfrak{a}) = \phi(a_0)\mathfrak{a}$. This shows $a_0\mathfrak{b} = \phi(a_0)\mathfrak{a}$. For the converse, we can assume $x\mathfrak{a} = y\mathfrak{b}$,

then $\forall \lambda \in \Lambda$, $\lambda \mathfrak{a} = (y/x)\mathfrak{b}$, where y/x is an element in the quotient field, one can check that it is indeed an isomorphism of Λ-module.

For the second statement, the Abelian multiplicative structure stems from the multiplicative structure of ideals. Furthermore, we can easily see that principal ideals belongs to a same ideal class because $a_0(b_0) = b_0(a_0)$. On the other hand, we have $\{(a_0)\}\{\mathfrak{b}\} = \{(a_0)\mathfrak{b}\}$ and $1 \cdot (a_0)\mathfrak{b} = a_0\mathfrak{b}$. $\qquad\square$

Proposition 1.18.

- *(1) Every ideal in a Dedekind domain Λ is finitely generated and projective.*

- *(2) Conversely , every fin gen projectives over Λ is isomorphic to a direct sum of ideals.*

Proof. (1) Take $\mathfrak{b} \neq 0$. Choose $0 \neq a_0 \in \mathfrak{b} \implies a_0\Lambda \subset \mathfrak{b}$. By the fact that it is Dedekind, $\exists \mathfrak{c}$ $s.t. a_0\Lambda = \mathfrak{c}\mathfrak{b}$ (we also know that $\mathfrak{c}$ is unique). $\implies \exists \{b_i\}_{i=1,...,k} \subset \mathfrak{b}, \{c_i\}_{i=1,...,k} \subset \mathfrak{c} : a_0 = \sum_i b_i c_i$. Define the Λ-linear mappings

$$\phi : \mathfrak{b} \longrightarrow \Lambda^k$$
$$b \mapsto (bc_1/a_0, ..., bc_k/a_0)$$
$$\varphi : \Lambda^k \longrightarrow \mathfrak{b}$$
$$(x_1, ..., x_k) \mapsto b_1 x_1 + ... + b_k x_k.$$

Since the composition is identify map of $\mathfrak{b}$, this proves that $\mathfrak{b}$ is finitely generated and projective. (It is finitely generated by $b_1, ..., b_k$ and projective because $Ker(\varphi) \oplus \mathfrak{b} \equiv \Lambda^k$).

(2) Any finitely generated projective P can be embedded in the free module Λ^k for some k. Projecting to the $k-th$ factor we obtain a homomorphism $\phi : P \to \Lambda$ with $(kernel(\phi) \subset \Lambda^{k-1}$. Since the image $\phi(P) = \mathfrak{a}_k$ is an ideal, hence projective, we have $P \cong (Ker(\phi)) \oplus \mathfrak{a}_k$. Again, we know $Ker(\phi)$ is a projective module, thus a induction conclude the theorem. $\qquad\square$

2 October 2nd

Theorem 2.1. *(Steinitz) Two direct sums $\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_r$ and $\mathfrak{b}_1 \oplus ... \oplus \mathfrak{b}_k$ are isomorphic as Λ-module iff $r = s$ and the ideal class $\{\mathfrak{a}_1...\mathfrak{a}_k\} = \{\mathfrak{b}_1...\mathfrak{b}_k\}$*

Proof. "$\Longrightarrow$", for this part we only need to assume Λ a integral domain.

Claim-1 If $\mathfrak{a} \subset \Lambda$ a nonzero ideal, then Λ-linear mapping $\phi : \mathfrak{a} \to \mathfrak{b} \subset \Lambda$, there is a unique $q \in Quot(\Lambda)$ s.t.

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

To prove this, it is only necessary to divide the equation $a_0\phi(a) = \phi(a_0 a) = \phi(a_0)a$ by a_0 setting $\phi(a_0)/a_0$, this is independent of the choice of a_0.

Then by the Claim-1, we have the Λ-linear mapping

$$\mathfrak{a}_1 \oplus .... \oplus \mathfrak{a}_r \to \mathfrak{b}_1 \oplus ... \oplus \mathfrak{b}_s$$

can be represented by a unique $s \times r$ matrix $Q = (q_{ij})$ with entries in the quotient field so that the

$$b_i = \sum q_{ij}a_j, \ \forall(a_1, ..., a_r) \in \mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_r,$$

because when we restrict to each entries, $\phi|_{\mathfrak{a}_j \mapsto \mathfrak{b}_i}$ is still a morphism of Λ-module. If ϕ is an isomorphism, then this matrix Q has an inverse, hence $r = s$.

Claim-2 $\mathfrak{b}_1..., \mathfrak{b}_r$ is equal to the $det(Q)\mathfrak{a}_1...\mathfrak{a}_r$. In fact, for each generator $a_1...a_r$ of $\mathfrak{a}_1...\mathfrak{a}_r$, the product $det(Q)a_1...a_r$ can be expressed as the determinant of the product matrix

$$Q \cdot \begin{pmatrix} a_1 & 0 & ... & 0 \\ 0 & a_2 & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & ... & a_r \end{pmatrix} = \begin{pmatrix} q_{11}a_1 & q_{12}a_2 & ... & q_{1r}a_r \\ q_{21}a_1 & q_{22}a_2 & ... & q_{2r}a_r \\ \vdots & \vdots & \ddots & \vdots \\ q_{r1}a_1 & q_{r2}a_2 & ... & q_{rr}a_r \end{pmatrix}.$$

Each entry of the of the i-th row of the product matrix belongs to $\mathfrak{b}_i$, hence the determinant of the product matrix is an element in $\mathfrak{b}_1...\mathfrak{b}_r$. Then we have

$$det(Q)\mathfrak{a}_1...\mathfrak{a}_r \subset \mathfrak{b}_1...\mathfrak{b}_r,$$

and similarly,

$$\mathfrak{a}_1...\mathfrak{a}_r \supset det(Q^{-1})\mathfrak{b}_1...\mathfrak{b}_r.$$

Then we get the Claim-2. By claim-2, we know $\{\mathfrak{a}_1...\mathfrak{a}_r\} = \{\mathfrak{b}_1...\mathfrak{b}_r\}$.

For the "$\Longleftarrow$" part, it suffice to prove that rank r and the ideal class $\{\mathfrak{a}_1...\mathfrak{a}_r\}$ form a complete invariant for $\mathfrak{a}_1 \oplus .... \oplus \mathfrak{a}_r$. Luckily, we have the following theorem, (of which the proof will be postponed)

Lemma 2.2. *If $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals in a Dedekind domain Λ, then the module $\mathfrak{a} \oplus \mathfrak{b}$ is isomorphic to $\Lambda^1 \oplus (\mathfrak{a}\mathfrak{b})$.*

With the Lemma 2.2, we can conclude

$$\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_r \cong \Lambda^{r-1} \oplus (\mathfrak{a}_1...\mathfrak{a}_r),$$

which indicate the "$\Longleftarrow$" part the theorem.

If we assume $\{\mathfrak{a}_1...\mathfrak{a}_r\} = \{\mathfrak{b}_1...\mathfrak{b}_s\}$, then by Proposition 1.17, we know $(\mathfrak{a}_1...\mathfrak{a}_r)$ is isomorphic to $(\mathfrak{b}_1...\mathfrak{b}_s)$ as Λ-modules, which implies

$$\mathfrak{a}_1 \oplus ... \oplus \mathfrak{a}_r \cong \Lambda^{r-1} \oplus (\mathfrak{a}_1...\mathfrak{a}_r) \cong \Lambda^{s-1} \oplus (\mathfrak{b}_1...\mathfrak{b}_s) \cong \mathfrak{b}_1 \oplus ... \oplus \mathfrak{b}_s.$$

The second isomorphism is only possible when $r = s$. $\qquad\square$

Now we come back to the proof of Lemma 2.2
Consider the **special case** if $\mathfrak{a}$ and $\mathfrak{b}$ happens to be relatively prime, then we know $\mathfrak{a} + \mathfrak{b} = \Lambda$. Map $\mathfrak{a} \oplus \mathfrak{b}$ onto Λ^1 by the correspondence $a \oplus b \mapsto a + b$. The kernel is clearly isomorphic to $\mathfrak{a} \cap \mathfrak{b}$. And since Λ^1 is projective, the exact 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 $\mathfrak{a} \cap \mathfrak{b}$ is just $\mathfrak{a}\mathfrak{b}$ when the two ideals are coprime.($1 \in \mathfrak{a} + \mathfrak{b} \Longrightarrow 1 = a_0 + b_0, \Longrightarrow \forall x \in \mathfrak{a} \cap \mathfrak{b}, x = a_0 x + b_0 x \in \mathfrak{a}\mathfrak{b}$. and the converse inclusion is always trivial.)

Then we can reduce the general case to the special case by the following Lemma:

Lemma 2.3. *Given nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a Dedekind domain Λ, there exists an ideal $\mathfrak{a}' \in \{\mathfrak{a}\}$ s.t. $\mathfrak{a}'$ and $\mathfrak{b}$ are relative prime.*

To prove the Lemma, we have to first introduce two of the standard properties of Dedekind domains.

Lemma 2.4. *Every nonzero ideal in a Dedekind domain can be expressed uniquely as a product of maximal ideals.*

Proof. **Existence:** $\mathfrak{a}$ not maximal $\Longrightarrow \mathfrak{a} \subset \mathfrak{m}_1$, then $\mathfrak{a} = \mathfrak{m}_1\mathfrak{a}_1$ for some ideal $\mathfrak{a}_1$, then similarly $\mathfrak{a}_1 = \mathfrak{m}_2\mathfrak{a}_2$ an so on with $\mathfrak{a} \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq ....$ This sequence must terminate because Λ is Noetherian.

Uniqueness: Assume $\mathfrak{m}_1...\mathfrak{m}_k = \tilde{\mathfrak{m}}_1...\tilde{\mathfrak{m}}_l$, then $\tilde{\mathfrak{m}}_1 \supset \mathfrak{m}_1...\mathfrak{m}_k$ and hence, since $\tilde{\mathfrak{m}}_1$ is prime, $\tilde{\mathfrak{m}}_1$ contains some $\mathfrak{m}_i$, and therefore is equal to $\mathfrak{m}_i$. We can get the uniqueness via the induction on $\max\{k, l\}$. For $\max\{k, l\} = 1$ the uniqueness is trivial. For $\max\{k, l\} = n$, we reduce it to $\mathfrak{m}_1(\mathfrak{m}_2...\mathfrak{m}_k) = \mathfrak{m}_1(\tilde{\mathfrak{m}}_1...\tilde{\mathfrak{m}}_{\hat{i}}...\tilde{\mathfrak{m}}_l)$, then we conclude $\mathfrak{m}_2...\mathfrak{m}_k = \tilde{\mathfrak{m}}_1...\tilde{\mathfrak{m}}_{\hat{i}}...\tilde{\mathfrak{m}}_l$ by Remark 1.15, which reduces to the induction steps of $\max\{k, l\} = n - 1$. $\qquad\square$

Remark 2.5. $\mathfrak{a}$ *is only included in finitely many maximals.*

Lemma 2.6. $\mathfrak{a}$ *nonzero ideal in Dedekind domain* Λ*,* $\Lambda/\mathfrak{a}$ *is* ***principal ideal ring****(usually with zero divisors)*

Proof. $\bar{I} \subset \Lambda/\mathfrak{a}$ is an ideal in $\Lambda/\mathfrak{a} \Longrightarrow I \subset \Lambda$, then we have $\mathfrak{a} \subset I = \mathfrak{m}_1...\mathfrak{m}_q$. Choose an element $x_1 \in \mathfrak{m}_1 \backslash \mathfrak{m}_1^2$ (by Lemma 2.4, $\mathfrak{m}_1^2 \subsetneq \mathfrak{m}_1$). The ideals $\mathfrak{m}_1, \mathfrak{m}_2, ..., \mathfrak{m}_q$ are pairwise relative prime $\Longrightarrow \mathfrak{m}_1^2, \mathfrak{m}_2, ..., \mathfrak{m}_q$ are pairwise relative prime. Then, by Chinese remainder theorem:

$$\frac{\Lambda}{(\mathfrak{m}_1^2...\mathfrak{m}_q)} \cong \frac{\Lambda}{\mathfrak{m}_1^2} \prod_{i=2}^{q} \frac{\Lambda}{\mathfrak{m}_i} \cong \frac{\Lambda}{\mathfrak{m}_1} \frac{\mathfrak{m}_1}{\mathfrak{m}_1^2} \prod_{i=2}^{q} \frac{\Lambda}{\mathfrak{m}_i}$$

there exists an element $y \in \Lambda$ s.t.

$$y_1 \equiv x_1 \mod \mathfrak{m}_1^2$$
$$y_1 \equiv 1 \mod \mathfrak{m}_j \ \forall j > 1,$$

The ideal $\mathfrak{a} \subsetneq (y_1) + \mathfrak{a} \subset \mathfrak{m}_1$ but $(y_1) + \mathfrak{a}$ is not contained in $\mathfrak{m}_1^2$ and any other $\mathfrak{m}_j$, $j > 1$ it has to be $\mathfrak{m}_1$ it self by Lemma 2.4. This proves that $\mathfrak{m}_1$ is a principal ideal modulo $\mathfrak{a}$, but every ideal in $\Lambda/\mathfrak{a}$ is a product of maximal ideals, we conclude that every ideal in $\Lambda/\mathfrak{a}$ is principal. $\qquad\square$

We finally come back to the proof of Lemma 2.3.

Proof. (of Lemma 2.3) Given non-zero ideals $\mathfrak{a}$ and $\mathfrak{b}$, choose $0 \neq a_0 \in \mathfrak{a}$ and define $\mathfrak{c}$ by $\mathfrak{c}\mathfrak{a} = (a_0)$. Apply the Lemma 2.6 to the ideal $\mathfrak{c}$ modulo $\mathfrak{c}\mathfrak{b}$, we see that $\mathfrak{c}$ is generated as $(x_0) + \mathfrak{b}\mathfrak{c}$. Now multiply it by $\mathfrak{a}$ and then divide by a_0, we obtain

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

Clearly, $\mathfrak{a}x_0/a_0$ is an element in the ideal class $\{\mathfrak{a}\}$, thus we prove the Lemma 2.3. Some remarks inverse of ideals in fraction field should be added $\qquad\square$

Corollary 2.7. Λ *a Dedekind domain, then we have*

$$K_0\Lambda \cong \mathbb{Z} \oplus C(\Lambda)$$

Proof. Consider the morphism of Abelian groups

$$K_0\Lambda \longrightarrow \mathbb{Z} \oplus C(\Lambda)[a_1 \oplus ... \oplus a_r] \ \mapsto (r, \{a_1...a_r\})$$

¿¿¿¿¿¿¿¿¿¿¿4 $\qquad\square$

Example 2.8. • $\Lambda = \mathbb{Z}$, $K_0\Lambda = \mathbb{Z}$

 • $\Lambda = \mathbb{Z}[\xi_n]$, $K_0\Lambda = \mathbb{Z} \oplus C(\mathbb{Z}[\xi_n])$

Definition 2.9. *A Λ-module M is called **invertible** if $\exists N$ s.t. $\Lambda^1 = M \otimes N$ free generated over 1 element.*

Definition 2.10. *The **Picard group** is the set of isomorphism classes of invertible modules $Pic(\Lambda)$*

$$[M][N] = [M \otimes N] = [\Lambda^1]$$

3   October 09

Definition 3.1. *Let $\mathbb{F}$ be a finite extension of the field $\mathbb{Q}$ of rational numbers (It is an algebraic number field). An element of $\mathbb{F}$ is called an **algebraic integer** if it is the root of a monic polynomial with coefficients in $\mathbb{Z}$. ({the algebraic closure of $\mathbb{Z}$}$\cap\mathbb{F}$)*

Example 3.2. *ξ_n is a complex number of multiplicative order n, then the set of algebraic integers alg.int.$\mathbb{Q}(\xi_n) = \mathbb{Z}[\xi_n]$*

Theorem 3.3. *The set $\Lambda = \Lambda(\mathbb{F}) = $ alg.int.$(\mathbb{F})$ consisting of all algebraic integers in $\mathbb{F}$ is a Dedekind domain, with quotient field $\mathbb{F}$.*

Proof. To prove this theorem, we need to show $\Lambda = $ alg.int.$(\mathbb{F})$ is a Dedekind domain.

Let n be the degree of $\mathbb{F}$ over $\mathbb{Q}$, i.e. $[\mathbb{F}/\mathbb{Q}] = n$. We use the term **lattice** be mean an additive subgroup of $\mathbb{F}$ which has a finite basis. Thus every lattice $L \subset \mathbb{F}$ is a free abelian additive group of rank $\leq n$ (Because every every basis of free abelian group in $\mathbb{F}$ must be in fact $\mathbb{Q}$-linear independent) The product LL' of two lattices in $\mathbb{F}$ is the lattice generated by all products ll' with $l \in L, l' \in L'$.
The proof consists of the following steps:

  (i) **Λ is a ring and its quotient field is $\mathbb{F}$**

 (ii) **Λ is a lattice of rank n**

(iii) **Λ fulfills**

   a. **Λ is Noetherian**

b. All non-zero prime ideals are maximal (Krull dimension 1)

c. For $f \in \mathbf{Quot}(\Lambda)$ and $\mathfrak{a}$ a non-zero ideal with $f\mathfrak{a} \subset \mathfrak{a} \Longrightarrow f \in \Lambda$ (Integrally closed)

(iv) A domain satisfying iii. is Dedekind.

- **proof of (i). Λ is a ring**
  We need the following the following criterion for an element in the algebraic number field to be algebraic integer:

  Lemma 3.4. (Criterion for algebraic integer) *An element $f \in \mathbb{F}$ is an algebraic integer "$\Longleftrightarrow$" there exists a non-zero lattice $L \subset \mathbb{F}$ s.t. $fL \subset L$.*

  Proof. "$\Longrightarrow$" f is root of $x^k + a_{k-1}x^{k-1} + \ldots a_0$, define $L = \mathbb{Z}[f]$ $fL \subset L$.

  "$\Longleftarrow$" Given $L = \langle b_1, \ldots, b_k \rangle$, s.t. $fL \subset L$, then we can set

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

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

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

  It follows that f satisfies

  $$det \begin{pmatrix} f - a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & f - a_{22} & \ldots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \ldots & f - a_{kk} \end{pmatrix} = 0$$

  it is a monic polynomial with coefficients in $\mathbb{Z}$. Then we conclude the f is an algebraic integer. $\square$

  Then, we conclude that set set of algebraic integer Λ is closed under addition and multiplication,**(It is a ring)**. For if $\lambda, \lambda' \in \Lambda$, then there exists lattice L and L' s.t. $\lambda L \subset L$ and $\lambda'L' \subset L'$ respectively. Now the product lattice $L'' = LL'$ will satisfy $(\lambda + \lambda')L'' \subset L''$ and $\lambda\lambda'L'' \subset L''$.

- **Proof of (i).** $frac(\Lambda) = \mathbb{F}$

Lemma 3.5. $\forall f \in \mathbb{F}, \ \exists m \in \mathbb{N} \ s.t. \ mf \in \Lambda$

Proof. Take minimal polynomial of f (over $\mathbb{Q}$) and multiply to get $p \in \mathbb{Z}[X]$, which is not necessarily monic

$$p(X) = a_k X^k + ... + a_0, \ p(f) = 0$$

$$(a_k X^k) + a_{k-1}(a_k X)^{k-1} + ... + a_0(a_k)^{k-1}$$

then we just take $m = a_k$ $\qquad\square$

Corollary 3.6. *Quotient field of Λ is $\mathbb{F}$*

Proof. Λ is a subring of an algebraic number field $\mathbb{F}$, then it is still a integral domain. We have the inclusion $frac(\Lambda) \subset \mathbb{F}$. We consider the converse inclusion. If an element $f \in \mathbb{F}$, then by the above lemma $\exists m \in \mathbb{N}$, s.t. $mf = \lambda \in \Lambda$. Also we have $m \in \Lambda, \implies f = \lambda/m \in frac(\Lambda)$. $\qquad\square$

- **Proof of (ii)**
  Recall the trace function for a finite extension $\mathbb{F}/\mathbb{Q}$, $\mathbb{F}$ is a n-dimensional vector space over $\mathbb{Q}$. For $f \in \mathbb{F}$, we have the linear operator on $\mathbb{F}$, $m_f : \mathbb{F} \longrightarrow \mathbb{F}$, and we define

$$tr_{\mathbb{F}/\mathbb{Q}}(f) := tr(m_f).$$

In the case of separable extension of degree n. There are exactly n distinct field embeddings $\sigma_1, ..., \sigma_n$, fixing $\mathbb{Q}$, from $\mathbb{F}$ into a Galois extension $\mathbb{F}'$ of $\mathbb{Q}$ containing $\mathbb{F}$. If $\sigma \in Aut(\mathbb{F}'/\mathbb{Q})$, then $\sigma\sigma_1, ..., \sigma\sigma_n$ is a permutation of $\sigma_1, ..., \sigma_n$; so for each $f \in \mathbb{F}$,

$$tr_{\mathbb{F}/\mathbb{Q}}(f) = \sigma_1(f) + ... + \sigma_n(f)$$

lies in the fixed field $\mathbb{Q}$. So the trace map $tr_{\mathbb{F}/\mathbb{Q}}$ is $\mathbb{Q}$-linear. By linear independence of characters, $\sigma_1, ..., \sigma_n \neq 0$; so trace is surjective. (For detailed construction see GTM 211 p285)

Claim $tr_{\mathbb{F}/\mathbb{Q}}(\Lambda) = \mathbb{Z}$ because the trace map is $\mathbb{Q}$-linear, it maps algebraic integers in $\mathbb{F}$ to algebraic integers in $\mathbb{Q}$, which is just $\mathbb{Z}$

$$
\begin{array}{ccc}
\mathbb{F} & \xrightarrow{tr_{\mathbb{F}/\mathbb{Q}}} & \mathbb{Q} \\
\uparrow & & \uparrow \\
\Lambda & \xrightarrow{tr_{\mathbb{F}/\mathbb{Q}}} & \mathbb{Z}.
\end{array}
$$

Choose $\lambda_1, ..., \lambda_n$ basis of $\mathbb{F}$ over $\mathbb{Q}$, (as $\mathbb{Q}$-vector space). W.l.o.g. $\lambda_i \in \Lambda$ (by the Lemma 3.5) define: $T : \mathbb{F} \longrightarrow \mathbb{Q}^n$ and $T : f \mapsto (tr_{\mathbb{F}/\mathbb{Q}}(\lambda_1 f), ..., tr_{\mathbb{F}/\mathbb{Q}}(\lambda_n f))$. Then the $\mathbb{Q}$-linear function is bijective, and embeds Λ in the direct sum $\mathbb{Z} \oplus ... \oplus \mathbb{Z}$.

$$
\begin{array}{ccc}
\mathbb{F} & \xrightarrow{T \cong} & \mathbb{Q}^n \\
\uparrow & & \uparrow \\
\Lambda & \xhookrightarrow{T} & \mathbb{Z}^n.
\end{array}
$$

Therefore, Λ is a finitely generated additive group of rank n.

- **Proof of (iii)**
Consider an ideal $I \subset \Lambda$

Lemma 3.7. *I is a lattice of rank n*

Proof. $i \in \mathbb{F}$: $m_i : \mathbb{F} \to \mathbb{F}, f \mapsto i \cdot f$, and $m_i^{-1} = m_{i^{-1}}$. Consider the special case $i \in I$ and we restrict it to Λ

$$m_i|_\Lambda : \Lambda \longrightarrow I$$

it is injective. Then by the isomorphism theorem $\Lambda \cong Im(m_i|_\Lambda)$, then $rank(\Lambda) = rank(Im(m_i|_\Lambda))$. Also $Im(m_i|_\Lambda) \subset I \subset \Lambda$

$$rank(I) = rank(\Lambda) = n$$

$\square$

Corollary 3.8. *Λ/I is finite*

because $rank(\Lambda/I) = 0$,(it is cyclic), but it is finitely generated module over $\mathbb{Z}$, thus Λ/I is finite.

16

(iii)a. Then Λ is Noetherian. In fact, if $\mathfrak{a}$ is a non-zero ideal, then $\Lambda/\mathfrak{a}$ is finite, so there are only finitely many large ideals.

(iii)b. Every non-zero prime ideal of Λ is maximal. For the quotient ring $\Lambda/\mathfrak{p}$, being finite and no zero divisors, it must be a field.

(iii)b. If an element f in the quotient field of Λ satisfies $f\mathfrak{a} \subset \mathfrak{a}$ for some non-zero ideal $\mathfrak{a}$, then $f \in \Lambda$. i.e. Λ is integrally closed in its quotient field.

- (Proof of (iv)) Any domain satisfying (iii) is in fact a Dedekind domain.

  Observation: Every non-zero ideal in a commutative Noetherian ring contains a product of non-zero prime ideals. For if $\mathfrak{a}$ is itself prime, it is done. Otherwise, choosing ring elements λ and λ' not in $\mathfrak{a}$ s.t. $\lambda\lambda' \in \mathfrak{a}$, the two ideals $\mathfrak{a} + \lambda\Lambda$ and $\mathfrak{a} + \lambda'\Lambda$ 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. (The induction make sense because Λ is Noetherian)

  We want to show: Given nonzero ideals $\mathfrak{a} \subset \mathfrak{b}$ in Λ, there exists an ideal $\mathfrak{c}$ s.t. $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

  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 product of prime ideals so that $\mathfrak{p}_1, ..., \mathfrak{p}_r \subset \Lambda b$, with r minimal. Also choose a maximal ideal $\mathfrak{p} \supset \mathfrak{b}$. Then $\mathfrak{p}$ contains the product $\mathfrak{p}_1...\mathfrak{p}_r$, hence $\mathfrak{p}$ contains some $\mathfrak{p}_i$, w.l.o.g we assume $\mathfrak{p}_i = \mathfrak{p}_1$. The product $\mathfrak{p}_2...\mathfrak{p}_r$ is not contained in Λb, since r is minimal. There exists an element $c \in \mathfrak{p}_2...\mathfrak{p}_r$, with $c \notin \Lambda b$. Evidently

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

  Therefore

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

  even though the element $c/b \in \mathbb{F}$ does not belong to Λ. Consider the ideal

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

  in Λ. Since $c.b \notin \Lambda$, then we know that $\mathfrak{b}'$ is strictly larger than $\mathfrak{b}$. Therefore by the induction hypothesis, given ang $\mathfrak{a} \subset \mathfrak{b}$ the equation

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

has a solution $\mathfrak{c}'$. Setting

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

we have

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

as required.

This set $\mathfrak{c}$ is actually contained in Λ, since it satisfies the condition $\mathfrak{b}\mathfrak{c} \subset \mathfrak{b}$. This shows that Λ is Dedekind domain.

$\square$

Constructing projective modules

Notation If $f : \Lambda \longrightarrow \Lambda_1$ is a ring homomorphism and M is a left Λ-module, denote the induced left Λ_1-module $\Lambda_1 \otimes_\Lambda M$ by $f_\# M$. There is a canonical Λ-linear map $f_* : M \longrightarrow f_\# M$ denoted by $f_*(m) = 1 \otimes_\Lambda m$.

Now consider the commutative square of a ring homomorphism

$$\begin{array}{ccc}
\Lambda & \xrightarrow{\ i_1\ } & \Lambda_1 \\
\downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\
\Lambda_2 & \xrightarrow{\ j_2\ } & \Lambda'
\end{array}$$

satisfying the following hypothesis

1. Λ is the fibred product of Λ_1 and Λ_2 over Λ.

2. At least one of the two homomorphism j_1 and j_2 is surjective.

Construction: Given a projective module P_1 over Λ_1, a projective module P_2 over Λ_2 and given an isomorphism $h : j_{1\#}P_1 \to j_{2\#}P_2$ over Λ', Λ_1. Let $M(P_1, P_2, h)$ denote the subgroup of $P_1 \times P_2$ consisting of all pairs (p_1, p_2) with $h \circ j_{1*}(p_1) = j_{2*}(p_2)$

This construction yields a commutative square of additive groups

$$\begin{array}{ccc}
M & \longrightarrow & P_1 \\
\downarrow & & \downarrow{\scriptstyle h \circ j_{j*}} \\
P_2 & \xrightarrow{\ j_{2*}\ } & j_{2\#}P_2.
\end{array}$$

It satisfies the analogous of Hypothesis above (fibred product of additive groups and one of morphism surjective). Finally, we make M into a left Λ-module by setting

$$\lambda \cdot (p_1, p_2) := (i_1(\lambda) \cdot p_1, i_2(\lambda)p_2)$$

Theorem 3.9. *The module $M(P_1, P_2, h)$ is projective over Λ. Furthermore if P_1 and P_2 are finitely generated over Λ_1 and Λ_2 respectively, then $M(P_1, P_2, h)$ is finitely generated over Λ*

Theorem 3.10. *Every projective Λ-module is isomorphic to $M(P_1, P_2, h)$ for some suitably chosen P_1, P_2, h.*

Theorem 3.11. *The module P_1 and P_2 are naturally isomorphic to $i_{1\#}M$ and $i_{2\#}M$ respectively.*