IDEAL CLASSES AND RELATIVE INTEGERS

KEITH CONRAD

The ring of integers of a number field is free as a $\mathbf{Z}$-module. It is a module not just over $\mathbf{Z}$, but also over any intermediate ring of integers. That is, if $E \supset F \supset \mathbf{Q}$ we can consider $\mathcal{O}_E$ as an $\mathcal{O}_F$-module. Since $\mathcal{O}_E$ is finitely generated over $\mathbf{Z}$, it is also finitely generated over $\mathcal{O}_F$ (just a larger ring of scalars), but $\mathcal{O}_E$ may or may not have a basis over $\mathcal{O}_F$.

When we treat $\mathcal{O}_E$ as a module over $\mathcal{O}_F$, rather than over $\mathbf{Z}$, we speak about a *relative* extension of integers. If $\mathcal{O}_F$ is a PID then $\mathcal{O}_E$ will be a free $\mathcal{O}_F$-module, so $\mathcal{O}_E$ will have a basis over $\mathcal{O}_F$. Such a basis is called a *relative integral basis* for E over F. The next three examples illustrate some possibilities when $\mathcal{O}_F$ is not a PID.

Example 1. Let $F = \mathbf{Q}(\sqrt{-5})$ and $E = \mathbf{Q}(i, \sqrt{-5}) = F(i)$. Although $\mathcal{O}_F = \mathbf{Z}[\sqrt{-5}]$ is not a PID, $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module with relative integral basis $\{1, \frac{i+\sqrt{-5}}{2}\}$.

Example 2. Let $F = \mathbf{Q}(\sqrt{-15})$ and $E = \mathbf{Q}(\sqrt{-15}, \sqrt{26}) = F(\sqrt{26})$. Then $h(F) = 2$, so $\mathcal{O}_F$ is not a PID, but it turns out that $\mathcal{O}_E = \mathcal{O}_F \oplus \mathcal{O}_F\sqrt{26}$, so $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module.

Example 3. Let $F = \mathbf{Q}(\sqrt{-6})$ and $E = \mathbf{Q}(\sqrt{-6}, \sqrt{-3}) = F(\sqrt{-3})$. Then $h(F) = 2$, so $\mathcal{O}_F$ is not a PID, and it turns out that

$$\mathcal{O}_E = \mathcal{O}_F e_1 \oplus \mathfrak{p} e_2, \tag{1}$$

where $e_1 = \frac{1+\sqrt{-3}}{2}$, $e_2 = \frac{1}{\sqrt{-3}}$, and $\mathfrak{p} = (3, \sqrt{-6})$. (Although e_2 is not in $\mathcal{O}_E$, there isn't a problem with the direct sum decomposition (1) for $\mathcal{O}_E$ over $\mathcal{O}_F$ since the coefficients of e_2 run not over $\mathcal{O}_F$ but over the ideal $\mathfrak{p}$, which doesn't include 1, so $e_2 \notin \mathfrak{p}e_2$.) Equation (1) says that as an $\mathcal{O}_F$-module, $\mathcal{O}_E \cong \mathcal{O}_F \oplus \mathfrak{p}$. The ideal $\mathfrak{p}$ is not principal and this suggests $\mathcal{O}_E$ is not a free $\mathcal{O}_F$-module, although that does require an argument. To reinforce this point, $\mathfrak{p} \oplus \mathfrak{p}$ does not look like a free $\mathcal{O}_F$-module, since $\mathfrak{p}$ is not principal, but $\mathfrak{p} \oplus \mathfrak{p}$ has a second direct sum decomposition that admits an $\mathcal{O}_F$-basis, so a direct sum of two non-free modules can be free. We will see how in Example 9 below.

What we are after is a classification of finitely generated torsion-free modules over a Dedekind domain, which will then be applied in the number field setting to describe $\mathcal{O}_E$ as an $\mathcal{O}_F$-module. The extent to which $\mathcal{O}_E$ could fail to have an $\mathcal{O}_F$-basis will be related to ideal classes in F.

A technical concept we need to describe modules over a Dedekind domain is projective modules.

Definition 4. Let A be any commutative ring. An A-module P is called *projective* if every surjective linear map $f\colon M \twoheadrightarrow P$ from any A-module M onto P looks like a projection out of a direct sum: there is an isomorphism $h\colon M \cong P \oplus N$ for some A-module N such that $h(m) = (f(m), *)$ for all $m \in M$.

The isomorphism h is not unique. For example, taking $A = \mathbf{Z}$, $P = \mathbf{Z}$, and $M = \mathbf{Z} \oplus \mathbf{Z}$ with $f(a, b) = a - 2b$, we can use $h\colon M \to P \oplus \mathbf{Z}$ by $h(a, b) = (a - 2b, b)$ or $h(a, b) =$

$(a-2b, a-b)$. Each of these works since the first coordinate of $h(a,b)$ is $f(a,b)$ and h is obviously invertible.

The complementary summand N in the definition of a projective module is isomorphic to the kernel of f. Indeed, the condition $h(m) = (f(m), *)$ means $f(m) = 0$ if and only if $h(m)$ is in $\{0\} \oplus N$, which means h restricts to an isomorphism between $\ker f$ and $\{0\} \oplus N \cong N$.

It is easy to give examples of non-projective modules. For instance, if P is a projective A-module with n generators there is a surjective A-linear map $A^n \twoheadrightarrow P$, so $A^n \cong P \oplus Q$ for some A-module Q. When A is a domain, any submodule of A^n is torsion-free, so a finitely generated projective module over a domain is torsion-free. Therefore a finitely generated module over a domain that has torsion is not projective: $\mathbf{Z} \oplus \mathbf{Z}/(2)$ is not a projective $\mathbf{Z}$-module. More importantly for us, though, is that fractional ideals in a Dedekind domain are projective modules.

Lemma 5. *For a domain A, any invertible fractional A-ideal is a projective A-module. In particular, when A is a Dedekind domain all fractional A-ideals are projective A-modules.*

Proof. Let $\mathfrak{a}$ be an invertible fractional A-ideal. Then $\sum_{i=1}^k x_i y_i = 1$ for some $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{a}^{-1}$. For each $x \in \mathfrak{a}$,

$$x = 1 \cdot x = x_1(x_1' x) + \cdots + x_k(x_k' x)$$

and $x_i' x \in \mathfrak{a}^{-1}\mathfrak{a} = A$, so $\mathfrak{a} \subset \sum_{i=1}^k Ax_i \subset \mathfrak{a}$, so $\mathfrak{a} = Ax_1 + \cdots + Ax_k$. In a similar way, $\mathfrak{a}^{-1} = Ay_1 + \cdots + Ay_k$. Suppose $f\colon M \twoheadrightarrow \mathfrak{a}$ is a surjective A-linear map. Choose $m_i \in M$ such that $f(m_i) = x_i$. Define $g\colon \mathfrak{a} \to M$ by $g(x) = \sum_{i=1}^k (xy_i)m_i$. Note $xy_i \in \mathfrak{a}\mathfrak{a}^{-1} = A$ for all i, so $g(x)$ makes sense and g is A-linear. Then

$$f(g(x)) = \sum_{i=1}^k (xy_i) f(m_i) = \sum_{i=1}^n (xy_i) x_i = x \sum_{i=1}^n x_i y_i = x.$$

Check the A-linear map $h\colon M \to \mathfrak{a} \oplus \ker f$ given by the formula $h(m) = (f(m), m - g(f(m)))$ has inverse $(x, y) \mapsto g(x) + y$. ■

Here is the main structure theorem.

Theorem 6. *Every finitely generated torsion-free module over a Dedekind domain A is isomorphic to a direct sum of ideals in A.*

Proof. Let M be a finitely generated torsion-free A-module. We can assume $M \neq 0$ and will show there is an embedding $M \hookrightarrow A^d$ for some $d \geqslant 1$ such that the image of M intersects each standard coordinate axis of A^d.

Let F be the fraction field of A and $x_1, \ldots, x_n$ be a generating set for M as an A-module. We will show n is an upper bound on the size of any A-linearly independent subset of M. Let $f\colon A^n \to M$ be the linear map where $f(e_i) = x_i$ for all i. (By $e_1, \ldots, e_n$ we mean the standard basis of A^n.) Let $y_1, \ldots, y_k$ be linearly independent in M, so their A-span is isomorphic to A^k. Write $y_j = \sum_{i=1}^n a_{ij} x_i$ with $a_{ij} \in A$. We pull the y_j's back to A^n by setting $v_j = (a_{1j}, \ldots, a_{nj})$, so $f(v_j) = y_j$. A linear dependence relation on the v_j's is transformed by f into a linear dependence relation on the y_j's, which is a trivial relation by their linear independence. Therefore $v_1, \ldots, v_k$ is A-linearly independent in A^n, hence F-linearly independent in F^n. By linear algebra over fields, $k \leqslant n$.

From the bound $k \leqslant n$, there is a linearly independent subset of M with maximal size, say $t_1, \ldots, t_d$. Then $\sum_{j=1}^d At_j \cong A^d$ by identifying t_j with the jth standard basis vector in A^d. We will find a scalar multiple of M inside $\sum_{j=1}^d At_j$. For any $x \in M$, the set $\{x, t_1, \dots, t_d\}$ is linearly dependent by maximality of d, so there is a nontrivial linear relation $a_x x + \sum_{i=1}^d a_i t_i = 0$, necessarily with $a_x \neq 0$ in A. Thus $a_x x \in \sum_{j=1}^d At_j$. Letting x run through the spanning set $x_1, \dots, x_n$, we have $ax_i \in \sum_{j=1}^d At_j$ for all i where $a = a_{x_1} \cdots a_{x_n} \neq 0$. Thus $aM \subset \sum_{j=1}^d At_j$. Multiplying by a is an isomorphism of M with aM, so we have the sequence of A-linear maps

$$M \to aM \hookrightarrow \sum_{j=1}^d At_j \to A^d,$$

where the first and last maps are A-module isomorphisms. In the above composite map, $t_j \in M$ is mapped to ae_j in A^d, so this composite map is an embedding $M \hookrightarrow A^d$ such that M meets each standard coordinate axis of A^d in a nonzero vector. Compose this linear map with projection $A^d \to A$ onto the last coordinate in the standard basis:

$$a_1 e_1 + \cdots + a_d e_d \mapsto a_d.$$

Denote the restriction of this to a map $M \to A$ as φ, so $\mathfrak{a} := \varphi(M)$ is a *nonzero* ideal in A. With φ we get a surjective map $M \twoheadrightarrow \mathfrak{a}$, so Lemma 5 (the first time we need A to be a Dedekind domain, not just an integral domain) tells us $M \cong \mathfrak{a} \oplus \ker \varphi$. Obviously $\ker \varphi \subset A^{d-1} \oplus 0 \cong A^{d-1}$, so $\ker \varphi$ is a finitely generated (and torsion-free) A-module with at most $d-1$ A-linearly independent elements. Using induction on the largest number of linearly independent elements in the module, $\ker \varphi$ is a direct sum of ideals in A. ∎

Remark 7. Using equations rather than isomorphisms, Theorem 6 says $M = M_1 \oplus \cdots \oplus M_d$ where each M_i is isomorphic to an ideal in A. Those ideals need not be principal, so M_i need not have the form Am_i. If M is inside a vector space over the fraction field of A, then $M = \bigoplus_{i=1}^d \mathfrak{a}_i e_i$ for some linearly independent e_i's, but be careful: if $\mathfrak{a}_i$ is a proper ideal in A then e_i is not in M since $1 \notin \mathfrak{a}_i$. The e_i's are *not* a spanning set for M as a module since their coefficients are not running through A. The decomposition of the integers of $\mathbf{Q}(\sqrt{-6}, \sqrt{-3})$ as a module over $\mathbf{Z}[\sqrt{-6}]$ in Example 3 illustrates this point.

How much does a direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_d$, as a module, depend on the individual $\mathfrak{a}_i$'s?

Lemma 8. *Let A be a Dedekind domain. For fractional A-ideals $\mathfrak{a}$ and $\mathfrak{b}$, there is an A-module isomorphism $\mathfrak{a} \oplus \mathfrak{b} \cong A \oplus \mathfrak{ab}$.*

Proof. Both sides of the isomorphism are unchanged up to A-module isomorphism when we scale $\mathfrak{a}$ and $\mathfrak{b}$, so without loss of generality $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals in A. We can further scale so $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Indeed, let $\mathfrak{a}^{-1} \sim \mathfrak{a}_0$ where $\mathfrak{a}_0 \subset A$. Using the Chinese remainder theorem in A, there is a nonzero ideal $\mathfrak{c}$ such that $\mathfrak{a}_0\mathfrak{c}$ is principal and $\gcd(\mathfrak{c}, \mathfrak{b}) = (1)$. Since $\mathfrak{c} \sim \mathfrak{a}_0^{-1} \sim \mathfrak{a}$, we can replace $\mathfrak{a}$ by $\mathfrak{c}$ without changing $\mathfrak{a} \oplus \mathfrak{b}$ or $A \oplus \mathfrak{ab}$ up to A-module isomorphism.

The linear map $f\colon \mathfrak{a} \oplus \mathfrak{b} \to \mathfrak{a} + \mathfrak{b} = A$ given by $f(a, b) = a - b$ is surjective and $\ker f = \{(a, a) : a \in \mathfrak{a} \cap \mathfrak{b}\} \cong \mathfrak{a} \cap \mathfrak{b}$, which is $\mathfrak{ab}$ since $\gcd(\mathfrak{a}, \mathfrak{b}) = (1)$. Applying Lemma 5 to the fractional A-ideal A, $\mathfrak{a} \oplus \mathfrak{b} \cong A \oplus \ker f \cong A \oplus \mathfrak{ab}$. ∎

Example 9. For $A = \mathbf{Z}[\sqrt{-5}]$, let $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$, so $\mathfrak{p}_2$ is not principal but $\mathfrak{p}_2^2 = 2A$ is principal. Then there is an A-module isomorphism $\mathfrak{p}_2 \oplus \mathfrak{p}_2 \cong A \oplus \mathfrak{p}_2^2 \cong A \oplus A$. That is intriguing: $\mathfrak{p}_2$ does not have an A-basis but $\mathfrak{p}_2 \oplus \mathfrak{p}_2$ does! Working through the proof of

Lemma 8 will show you how to write down a basis of $\mathfrak{p}_2 \oplus \mathfrak{p}_2$ explicitly. In a similar way, $\mathfrak{p} \oplus \mathfrak{p}$ in Example 3 is a free $\mathbf{Z}[\sqrt{-6}]$-module since $\mathfrak{p}^2$ is principal.

Theorem 10. *Let A be a Dedekind domain. For fractional A-ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_d$, there is an A-module isomorphism $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_d \cong A^{d-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_d$.*

Proof. Induct on d and use Lemma 8. ∎

Corollary 11. *Let E/F be a finite extension of number fields with $[E : F] = n$. As an $\mathcal{O}_F$-module, $\mathcal{O}_E \cong \mathcal{O}_F^{n-1} \oplus \mathfrak{a}$ for some nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_F$.*

Proof. Since $\mathcal{O}_E$ is a finitely generated $\mathbf{Z}$-module it is a finitely generated $\mathcal{O}_F$-module and obviously has no torsion, so Theorems 6 and 10 imply $\mathcal{O}_E \cong \mathcal{O}_F^{d-1} \oplus \mathfrak{a}$ for some $d \geqslant 1$ and nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_F$. Letting $m = [F : \mathbf{Q}]$, both $\mathcal{O}_F$ and $\mathfrak{a}$ are free of rank m over $\mathbf{Z}$, while $\mathcal{O}_E$ is free of rank mn over $\mathbf{Z}$. Computing the rank of $\mathcal{O}_E$ and $\mathcal{O}_F^{d-1} \oplus \mathfrak{a}$ over $\mathbf{Z}$, $mn = m(d-1) + m = md$, so $d = n$. ∎

Thus $\mathcal{O}_E$ is almost a free $\mathcal{O}_F$-module. If $\mathfrak{a}$ is principal then $\mathcal{O}_E$ is free. As an $\mathcal{O}_F$-module up to isomorphism, $\mathcal{O}_F^{n-1} \oplus \mathfrak{a}$ only depends on $\mathfrak{a}$ through its ideal class, since $\mathfrak{a}$ and any $x\mathfrak{a}$ ($x \in F^\times$) are isomorphic $\mathcal{O}_F$-modules. Does $\mathcal{O}_F^{n-1} \oplus \mathfrak{a}$, as an $\mathcal{O}_F$-module, depend on $\mathfrak{a}$ exactly through its ideal class? That is, if $\mathcal{O}_F^{n-1} \oplus \mathfrak{a} \cong \mathcal{O}_F^{n-1} \oplus \mathfrak{b}$ as $\mathcal{O}_F$-modules, does $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathrm{Cl}(F)$? The next two theorems together say the answer is yes.

Theorem 12. *Let A be a domain with fraction field F. For fractional A-ideals $\mathfrak{a}$ and $\mathfrak{b}$ in F, $\mathfrak{a} \cong \mathfrak{b}$ as A-modules if and only if $\mathfrak{a} = x\mathfrak{b}$ for some $x \in F^\times$.*

Here F is any field, not necessarily a number field.

Proof. ($\Leftarrow$): Multiplication by x is an A-module isomorphism from $\mathfrak{b}$ to $\mathfrak{a}$.

($\Rightarrow$): Suppose $f\colon \mathfrak{a} \to \mathfrak{b}$ is an A-module isomorphism. We want an $x \in F^\times$ such that $f(t) = xt$ for all $t \in \mathfrak{a}$. For this to be possible, $f(t)/t$ has to be independent of the choice of nonzero t. Then we could define x to be this common ratio, so $f(t) = xt$ for all t in $\mathfrak{a}$ (including $t = 0$).

For any nonzero t_1 and t_2 in $\mathfrak{a}$,

$$\frac{f(t_1)}{t_1} \stackrel{?}{=} \frac{f(t_2)}{t_2} \iff t_2 f(t_1) \stackrel{?}{=} t_1 f(t_2).$$

You may be tempted to pull the t_2 and t_1 inside on the right, confirming the equality, but that is bogus because f is A-linear and we don't know if t_1 and t_2 are in A (they are just in F). This is easy to fix. Since $\mathfrak{a}$ is a fractional A-ideal, it has a denominator: $d\mathfrak{a} \subset A$ for some nonzero $d \in A$. Then $dt_1, dt_2 \in A$, so

$$t_2 f(t_1) \stackrel{?}{=} t_1 f(t_2) \iff dt_2 f(t_1) \stackrel{?}{=} dt_1 f(t_2) \iff f(dt_2 t_1) \stackrel{\checkmark}{=} f(dt_1 t_2).$$

∎

Theorem 13. *For nonzero ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ and $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ in a Dedekind domain A,we have $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \cong \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ as A-modules if and only if $m = n$ and $[\mathfrak{a}_1 \cdots \mathfrak{a}_m] = [\mathfrak{b}_1 \cdots \mathfrak{b}_n]$ in $\mathrm{Cl}(A)$.*

Proof. The "if" direction follows from Theorems 10 and 12: $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \cong A^{m-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_m$, so if $m = n$ and $[\mathfrak{a}_1 \cdots \mathfrak{a}_m] = [\mathfrak{b}_1 \cdots \mathfrak{b}_m]$ in $\mathrm{Cl}(A)$ then

$$A^{m-1} \oplus \mathfrak{a}_1 \cdots \mathfrak{a}_m \cong A^{m-1} \oplus \mathfrak{b}_1 \cdots \mathfrak{b}_m \cong \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_m.$$

Turning to the "only if" direction, we show m is determined by the A-module structure of $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$: it is the largest number of A-linearly independent elements in this module. Picking a nonzero $a_i \in \mathfrak{a}_i$, the m-tuples $(\dots, 0, a_i, 0, \dots)$ for $1 \leqslant i \leqslant m$ are easily A-linearly independent, so $\bigoplus_{i=1}^m \mathfrak{a}_i$ has m linearly independent members. Since $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \subset F^m$, where F is the fraction field of A, any set of more than m members of $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m$ has a nontrivial F-linear relation in F^m, which can be scaled to a nontrivial A-linear relation in $\bigoplus_{i=1}^m \mathfrak{a}_i$ by clearing a common denominator in the coefficients. Therefore if $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_m \cong \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ as A-modules we must have $m = n$ by computing the maximal number of A-linearly independent elements in both modules.

To show $\bigoplus_{i=1}^m \mathfrak{a}_i \cong \bigoplus_{i=1}^m \mathfrak{b}_i \Rightarrow \mathfrak{a}_1 \cdots \mathfrak{a}_m$ and $\mathfrak{b}_1 \cdots \mathfrak{b}_m$ are scalar multiples, we can collect ideals by multiplication into the last summands: it is enough to show $A^{m-1} \oplus \mathfrak{a} \cong A^{m-1} \oplus \mathfrak{b} \Rightarrow \mathfrak{a}$ and $\mathfrak{b}$ are scalar multiples. Let $\varphi\colon A^{m-1} \oplus \mathfrak{a} \to A^{m-1} \oplus \mathfrak{b}$ be an A-module isomorphism. Viewing $A^{m-1} \oplus \mathfrak{a}$ and $A^{m-1} \oplus \mathfrak{b}$ as column vectors of length m with the last coordinate in $\mathfrak{a}$ or $\mathfrak{b}$, φ can be represented as an $m \times m$ matrix of A-linear maps (φ_{ij}), where φ_{ij} has domain A or $\mathfrak{a}$ and target A or $\mathfrak{b}$. The proof of Theorem 12 shows any A-linear map from one fractional A-ideal to another (not necessarily injective or surjective) is a scaling function. Therefore φ is described by an $m \times m$ matrix of numbers, say $\mathcal{M}$, acting in the usual way on column vectors.

For any $\alpha \in \mathfrak{a}$, let $D_\alpha = \operatorname{diag}(1, \dots, 1, \alpha)$ be the diagonal $m \times m$ matrix with α in the lower right entry. Then $D_\alpha(A^{m-1} \oplus A) \subset A^{m-1} \oplus \mathfrak{a}$, so $\mathcal{M}D_\alpha$ maps $A^{m-1} \oplus A$ to $A^{m-1} \oplus \mathfrak{b}$. This means the bottom row of $\mathcal{M}D_\alpha$ has all entries in $\mathfrak{b}$, so $\det(\mathcal{M}D_\alpha) \in \mathfrak{b}$. Since D_α has determinant α and α is arbitrary in $\mathfrak{a}$, $\det(\mathcal{M})\mathfrak{a} \subset \mathfrak{b}$. In the same way, $\det(\mathcal{M}^{-1})\mathfrak{b} \subset \mathfrak{a}$, so $\det(\mathcal{M})\mathfrak{a} = \mathfrak{b}$. ∎

Example 14. Let's return to Example 3: $F = \mathbf{Q}(\sqrt{-6})$, $E = F(\sqrt{-3})$, and $\mathcal{O}_E \cong \mathcal{O}_F \oplus \mathfrak{p}$, where $\mathfrak{p} = (3, \sqrt{-6})$. We can show $\mathcal{O}_E$ is not a free $\mathcal{O}_F$-module: if it were free then $\mathcal{O}_E \cong \mathcal{O}_F^2$, so $\mathcal{O}_F \oplus \mathfrak{p} \cong \mathcal{O}_F \oplus \mathcal{O}_F$ as $\mathcal{O}_F$-modules. Then Theorem 13 implies $\mathfrak{p} \cong \mathcal{O}_F$ as $\mathcal{O}_F$-modules, so $\mathfrak{p}$ is principal, but $\mathfrak{p}$ is nonprincipal. This is a contradiction.

We can now associate to any finite extension of number fields E/F a canonical ideal class in $\mathrm{Cl}(F)$, namely $[\mathfrak{a}]$ where $\mathcal{O}_E \cong \mathcal{O}_F^{n-1} \oplus \mathfrak{a}$ as $\mathcal{O}_F$-modules. Theorem 13 assures us $[\mathfrak{a}]$ is well-defined. Since the construction of $[\mathfrak{a}]$ is due to Steinitz (1912), $[\mathfrak{a}]$ is called the *Steinitz class* of E/F.

Example 15. By Example 14, when $F = \mathbf{Q}(\sqrt{-6})$ the nontrivial member of $\mathrm{Cl}(F)$ is the Steinitz class of the quadratic extension $F(\sqrt{-3})/F$.

Since the ideal class group of a number field F is finite, as E varies over all extensions of F with a fixed degree $n \geqslant 2$ the different $\mathcal{O}_E$'s have finitely many possible $\mathcal{O}_F$-module structures, in fact at most $h(F)$ of them. There are infinitely many nonisomorphic extensions of F with degree n, so it is natural to ask if each ideal class is realized among them: for any $[\mathfrak{a}] \in \mathrm{Cl}(F)$ and integer $n \geqslant 2$ is there some extension E/F of degree n whose Steinitz class is $[\mathfrak{a}]$, *i.e.*, $\mathcal{O}_E \cong \mathcal{O}_F^{n-1} \oplus \mathfrak{a}$ as $\mathcal{O}_F$-modules?

The answer is yes for $n = 2, 3, 4$, and 5 [1] (see [2] for $n = 2$ and 3). More precisely, the field extensions E/F of degree n with Galois closure having Galois group S_n are equidistributed in terms of their Steinitz classes in $\mathrm{Cl}(F)$. In particular, each ideal class in $\mathrm{Cl}(F)$ is a Steinitz class for infinitely many nonisomorphic degree n extensions of F when $n = 2, 3, 4$, and 5. The extension to general degrees is still an open problem in general.

We have focused on the description of a single finitely generated torsion-free module over a Dedekind domain. What if we want to compare such a module and a submodule? If A

is a PID, M is a finite free A-module and M' is a submodule then we can align M and M' in the sense that there is a basis $e_1, \ldots, e_n$ of M and nonzero scalars $a_1, \ldots, a_m$ in A (where $m \leqslant n$) such that $M = \bigoplus_{i=1}^n Ae_i$ and $M' = \bigoplus_{j=1}^m Ae_j$. This has an analogue over Dedekind domains, but it doesn't use bases. If A is a Dedekind domain, M is a finitely generated torsion-free A-module, and M' is a submodule of M, then we can align M and M' in the sense that we can write

$$M = \bigoplus_{i=1}^n M_i \qquad \text{and} \qquad M' = \bigoplus_{j=1}^m \mathfrak{a}_j M_j$$

where $m \leqslant n$, each M_i is isomorphic to a nonzero ideal in A, and each $\mathfrak{a}_j$ is a nonzero ideal in A. It is generally false that such an alignment is compatible with an isomorphism $M \cong A^{n-1} \oplus \mathfrak{a}$. That is, such an isomorphism need not restrict to M' to give an isomorphism $M' \cong A^{m-1} \oplus \mathfrak{a}'$ with $\mathfrak{a}' \subset \mathfrak{a}$, even for $A = \mathbf{Z}$. Consider, for instance, $M = \mathbf{Z} \oplus \mathbf{Z}$ and $M' = a\mathbf{Z} \oplus a\mathbf{Z}$ for $a > 1$ (so $m = n = 2$). We can't write $M = \mathbf{Z}e_1 \oplus \mathbf{Z}e_2$ and $M' = \mathbf{Z}e_1 \oplus b\mathbf{Z}e_2$ for some integer b since that would imply $M/M' \cong \mathbf{Z}/b\mathbf{Z}$ is cyclic, whereas $M/M' \cong (\mathbf{Z}/a\mathbf{Z})^2$ is not cyclic.

References

[1] M. Bhargava, A. Shankar, and X. Wang, Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces, preprint (2015), https://arxiv.org/abs/1512.03035.

[2] A. C. Kable and D. J. Wright, Uniform distribution of the Steinitz invariants of quadratic and cubic extensions, *Compositio Math.* **142** (2006), 84–100.