

2009 REU: QUADRATIC FIELDS

1. MODULES AND ORDERS

Let K be a finite extension, say of degree n , of \mathbb{Q} . A \mathbb{Z} -submodule of K is called *full* if its rank is n . In other words, M is a \mathbb{Z} -span of a basis $(\alpha_1, \dots, \alpha_n)$ of K over \mathbb{Q} . We shall denote this as $M = \{\alpha_1, \dots, \alpha_n\}$. A full module which is, in addition, a ring with 1 is called an *order*. For any full module M , an element α in K such that $\alpha M \subseteq M$ is a multiplier of M . The set of all multipliers of M is clearly a ring, which will be denoted by R . In a moment, we shall show that R is an order, but first, let us remark that if M is an order, then $R = M$. Indeed, $R \subseteq M$, since 1 is in M , and $M \subseteq R$, since M is closed under the multiplication. In particular $R = M$, as desired.

Proposition 1.1. *Let M be a full module, and R its ring of multipliers. Then*

- R is a full module.
- R is contained in the ring of algebraic integers.

In particular, the ring of algebraic integers is called the maximal order in K .

Proof. Note that the ring of multipliers does not change if we replace M by δM where $\delta \in K^\times$. In particular, we can assume that 1 is in M . This implies that $R = R \cdot 1 \subseteq M$. Let $(\alpha_1, \dots, \alpha_n)$ be a \mathbb{Z} -basis of M . Let A_{α_i} be the rational matrix expressing the multiplication by α_i in the basis $(\alpha_1, \dots, \alpha_n)$. Let ℓ be a positive integer such that $\ell \cdot A_{\alpha_i}$ has integral coefficients. It follows that

$$\frac{1}{\ell}M \subseteq R \subseteq M.$$

In particular, R is an order. This proves the first statement. If γ is a multiplier of M then the matrix A_γ has integer coefficients. The characteristic polynomial of A_γ is a monic polynomial with integer coefficients. Since γ is a root of the characteristic polynomial it follows that it is an algebraic integer. The proposition is proved. \square

Let R be a fixed order. It is not difficult to see that any finitely generated R module $M \subseteq K$ is a full module. In particular, if M and N are two such R -modules, then MN is also a finitely generated R module.

Definition 1.2. *An R -module $M \subseteq K$ is called invertible, if $M^{-1}M = R$ where*

$$M^{-1} = \{x \in K \mid xM \subseteq R\}.$$

The set of invertible R -modules forms a group, denoted by $\mathcal{M}(R)$.

Proposition 1.3. *A finitely generated R -module $M \subseteq K$ is invertible if and only if it is projective.*

Proof. If M is invertible, then there exist elements m_i in M and x_i in M^{-1} such that $\sum x_i m_i = 1$. Let

$$\begin{array}{ccccc}
 & & M & & \\
 & \swarrow & \downarrow & & \\
 B & \longrightarrow & A & \longrightarrow & 0
 \end{array}$$

be a diagram of R -modules. To show that M is projective, we need to define $h : M \rightarrow B$ making the diagram commutative. To that end, let $a_i = f(m_i)$ and pick b_i in B such that $p(b_i) = a_i$. Since $m = \sum (mx_i)m_i$ for any m in M , and mx_i is in R , we can define h by

$$h(m) = \sum (mx_i)b_i.$$

Now assume that $M \subset K$ is projective. In order to prove that M is invertible it suffices to do it for any multiple δM . In particular, we can assume that M is contained in R . Since M is a finitely generated, there exist a surjective map $p : R^n \twoheadrightarrow M$. Consider the diagram

$$\begin{array}{ccccc}
 & & M & & \\
 & \swarrow & \downarrow & & \\
 R^m & \longrightarrow & M & \longrightarrow & 0
 \end{array}$$

of R -modules, where the vertical arrow is the identity. Since M is projective, there exist a map $h : M \rightarrow R^m$ making the diagram commutative. Let e_i be the standard basis vectors in R^m , and let $m_i = p(e_i)$. Let $h_i : M \rightarrow R$ be the i -th component of the map h , so that

$$h(m) = \sum h_i(m)e_i,$$

for every element m in M . It follows that $m = \sum h_i(m)m_i$ by commutativity of the diagram. If $m \neq 0$ we can rewrite this equation as

$$1 = \sum \frac{h_i(m)}{m} m_i = \sum x_i m_i$$

where $x_i = h_i(m)/m \in K$. We claim that x_i does not depend on m . Indeed, since h_i is a homomorphism of R -modules, and we assume that $M \subseteq R$,

$$mh_i(m') = h_i(mm') = m'h_i(m)$$

for any two elements m and m' in M . If m and m' are non-zero, then we can divide both sides by mm' , which proves that x_i is independent of m . It follows that $x_i m = h_i(m)$ for any $m \in M$. This shows that x_i is in M^{-1} . Since $1 = \sum x_i m_i$ the proposition is proved. \square

It follows that the set of projective R -modules forms a group, denoted by \mathcal{M} . Two modules are said to be similar if $M' = \delta M$ for some δ in K^\times . This defines an equivalence relation on \mathcal{M} and the group of equivalence classes will be denoted by $Pic(R)$. In other words, $Pic(R) = \mathcal{M}/[R]$ where $[R]$ is the class class of principal R -modules.

2. QUADRATIC FIELDS

As the title suggests we shall now specialize to quadratic extensions of \mathbb{Q} . Every quadratic extension K can be written as the set

$$K = \mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}.$$

where d is a square free integer. For every element $\alpha = x + y\sqrt{d}$, define the conjugate $\bar{\alpha} = x - y\sqrt{d}$, and the trace and the norm by

$$\begin{cases} \text{Tr}(\alpha) = \alpha + \bar{\alpha} = 2x \\ N(\alpha) = \alpha\bar{\alpha} = x^2 - dy^2. \end{cases}$$

Note that the trace and the norm are equal to the trace and the determinant of the linear map $A_\alpha(\beta) = \alpha\beta$, and that α is a root of $x^2 - \text{Tr}(\alpha)x + N(\alpha)$. Recall that α in K is an *algebraic integer* if this quadratic polynomial has integer coefficients.

Proposition 2.1. *Let d be a square free integer. Then the maximal order R_{\max} (the set of algebraic integers) in $\mathbb{Q}(\sqrt{d})$ is spanned, as a \mathbb{Z} -module, by 1 and*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod{4} \\ (1 + \sqrt{d})/2 & \text{and } d \equiv 1 \pmod{4}. \end{cases}$$

Proof. Let $\alpha = x + y\sqrt{d}$ be an algebraic integer, so that $\text{Tr}(\alpha)$ and $N(\alpha)$ are integers. Since $\text{Tr}(\alpha) = 2x$, it follows that x is either an integer or a half integer. Clearly, if x is a half integer, so is y . Therefore, assume that $x = m/2$ and $y = n/2$ for two odd integers m and n . Then

$$N(\alpha) = \frac{m^2 - n^2d}{4}.$$

Since $m^2 \equiv n^2 \equiv 1 \pmod{4}$, the above expression is an integer if and only if $d \equiv 1 \pmod{4}$. The proposition is proved. \square

Let $R = \{1, \tau\}$ be any order in K . Its *discriminant* D , is the determinant of the trace pairing. More precisely, in terms of the given basis,

$$D = \begin{vmatrix} \text{Tr}(1) & \text{Tr}(\tau) \\ \text{Tr}(\tau) & \text{Tr}(\tau^2) \end{vmatrix}.$$

It is easy to check that the discriminant of the maximal order $R_{\max} \subseteq \mathbb{Q}(\sqrt{d})$ is

$$D_{\max} = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod{4} \\ d & \text{and } d \equiv 1 \pmod{4}. \end{cases}$$

On the other hand, if R is any order, then $D = [R_{\max} : R]^2 D_{\max}$. It follows that the discriminant D can be congruent to 0 or 1 modulo 4 only! In fact, it is not difficult to see that the order R is determined by its discriminant D , and we can pick τ to be

$$\tau = \begin{cases} \sqrt{D}/2 & \text{if } D \equiv 0 \pmod{4} \\ (1 + \sqrt{D})/2 & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

In order to state results as neatly as possible, we shall work with *oriented* modules. Formally, an oriented module is a pair (M, ϵ) where ϵ is a sign. Two oriented modules are multiplied according to the rule

$$(M_1, \epsilon_1) \cdot (M_2, \epsilon_2) = (M_1 M_2, \epsilon_1 \epsilon_2).$$

In practical terms, the sign will specify orientation of a basis of M . More precisely, a basis (α, β) of the oriented module is *proper* if it has the same orientation as $(1, \tau)$ and ϵ is positive, or it has the opposite orientation as $(1, \tau)$ and ϵ is negative. Two oriented modules are said to be similar, if $M' = \delta M$ and $\epsilon' = \text{sign}(N(\delta))\epsilon$. This defines an equivalence relation on the set of oriented modules. The corresponding classes will be called *narrow* classes.

Let (M, ϵ) be an oriented module. Let (α, β) be a basis with the proper orientation. The *norm* $N(M)$ of the oriented module is the determinant of the 2×2 matrix expressing the basis (α, β) in terms of the basis $(1, \tau)$. If M is contained in R , then

$$N(M) = \epsilon \cdot [R : M].$$

Also, note that $N(\delta M) = N(\delta)N(M)$. Define \mathcal{M}^+ to be the group of oriented, invertible, full \mathbb{Z} -modules with the multiplier ring R . The identity element of this group is $R^+ = (R, +)$. Let $\text{Pic}^+(R) = \mathcal{M}^+ / [R^+]$ where $[R^+]$ is the class class of principal R -modules. Note that $[R^+]$ consists of pairs $((\delta), \epsilon)$ where $(\delta) = \delta \cdot R$ is a principal module, and $\epsilon = \text{sign}(N(\delta))$. In particular, if there exists an element δ in R such that $N(\delta) = -1$, then the class $[R^+]$ contains $(R, -)$ and $\text{Pic}^+(R) = \text{Pic}(R)$. Otherwise $\text{Pic}^+(R) = \text{Pic}(R) \times \{\pm 1\}$.

Proposition 2.2. *Let $ax^2 + bx + c$ be a quadratic polynomial such that a, b and c are relatively prime integers. Assume that $D = b^2 - 4ac$ is not a square. Let*

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Consider the oriented module (M, ϵ) where $M = \{1, \gamma\}$, and $\epsilon = \text{sign}(a)$. Then the multiplier ring of M is the unique order of discriminant D , the basis $(1, \gamma)$ is proper and the norm $N(M)$ of (M, ϵ) is $1/a$.

Proof. Let $\alpha = x + y\gamma$ be in R , the multiplier ring. Since $\alpha \cdot 1$ and $\alpha \cdot \gamma$ are in M , it follows that

$$x, y, \frac{yc}{a} \text{ and } \frac{yb}{a}$$

are integers. Since a, b and c are relatively prime, it follows that a divides y . Thus, $R = \{1, a\gamma\}$. Now note that b is even if $D \equiv 0 \pmod{4}$ and odd if $D \equiv 1 \pmod{4}$. Thus, if we write

$$a\gamma = -\frac{b}{2} + \frac{\sqrt{D}}{2}$$

if $D \equiv 0 \pmod{4}$ and

$$a\gamma = -\frac{b+1}{2} + \frac{1+\sqrt{D}}{2}$$

if $D \equiv 1 \pmod{4}$, we see that $R = \{1, \tau\}$. Next, the matrix of the basis $(1, \gamma)$ of M in terms of the basis $(1, \tau)$ is

$$\begin{pmatrix} 1 & * \\ 0 & \frac{1}{a} \end{pmatrix}.$$

The determinant of this matrix is $1/a$ which shows, both, that the basis $(1, \gamma)$ is proper and $N(M) = 1/a$. □

We shall now describe the group \mathcal{M} in more details. The key is the following proposition which shows that any full module M with R as its multiplier ring is invertible.

Proposition 2.3. *Let (M, ϵ) be an oriented full module such that its ring of multipliers is R . Then $M \cdot \bar{M} = N(M)R$. In particular, M is invertible, and the oriented inverse of (M, ϵ) is $(\frac{1}{N(M)}\bar{M}, \epsilon)$.*

Proof. We can assume that $M = \{1, \gamma\}$, by rescaling M , if necessary. There is a unique polynomial $ax^2 + bx + c$, with relatively prime integer coefficients, such that

$$\gamma = \frac{-b + \sqrt{D}}{2a},$$

where $D = b^2 - 4ac$. Note that D must be the discriminant of R , by the previous proposition. Note that $N(M) = 1/a$ or $-1/a$ depending whether $(1, \gamma)$ is proper or not. This is not important here. The product $M \cdot \bar{M}$ is generated by $1, \gamma, \bar{\gamma}$ and $\gamma\bar{\gamma}$. Since

$$\gamma + \bar{\gamma} = -\frac{b}{a} \text{ and } \gamma\bar{\gamma} = \frac{c}{a}$$

we see that $aM\bar{M}$ is generated by a, b, c and $a\gamma$. Since a, b and c are relatively prime, we can replace them by 1. It follows that $aM\bar{M} = \{1, a\gamma\} = R$. Since $N(M) = \pm 1/a$, the proposition follows. □

Corollary 2.4. *Let (M, ϵ) and (N, ϵ') be two oriented, full modules with the same multiplier ring R . Then $N(MN) = N(M)N(N)$.*

Proof. Note that the conjugate of $M \cdot N$ is $\bar{N} \cdot \bar{M}$. The proposition implies that

$$(MN)(\bar{N}\bar{M}) = (M\bar{M})(N\bar{N}) = N(M)N(N) \cdot R$$

and

$$(MN)(\bar{N}\bar{M}) = (MN)(\overline{MN}) = N(MN) \cdot R.$$

This shows that $N(M)N(N) = \pm N(MN)$. Since, by definition, the sign of $N(M)$ is ϵ , the sign of $N(N)$ is ϵ' and the sign of $N(MN)$ is $\epsilon\epsilon'$, the signs must also match. The corollary is proved. □

Theorem 2.5. *The set \mathcal{M} of all full oriented modules with the multiplier ring of discriminant D is a commutative group under the operation \cdot , with $(R, +)$ as a unit, and inverse defined by*

$$(M, \epsilon)^{-1} = \left(\frac{1}{N(M)}\bar{M}, \epsilon\right).$$

3. QUADRATIC FORMS

Recall that a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is primitive if a, b and c are relatively prime integers. The discriminant of Q is $D = b^2 - 4ac$.

Let R be the (unique) quadratic order of discriminant D . We shall now build a correspondence between oriented, full modules with the multiplier ring R and primitive quadratic forms of discriminant D .

Let M be an oriented full module. Pick a proper basis (α, β) of M . Define

$$Q_M(x, y) = \frac{1}{N(M)} N(x\alpha - y\beta).$$

Note that the form Q_M does not change if we replace the triple $(M, (\alpha, \beta), \epsilon)$ by any non-zero multiple $(M', (\alpha', \beta'), \epsilon')$ where $M' = \delta M$, $\alpha' = \delta\alpha$, $\beta' = \delta\beta$ and $\epsilon' = \epsilon \cdot \text{sign}(N(\delta))$. In particular, in order to calculate Q_M , we can assume that the triple is $(M, (1, \gamma), \epsilon)$. Let $ax^2 + bx + c$ be the (unique) polynomial such that a, b and c are relatively prime integers and such that

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Since $(1, \gamma)$ is a proper basis, the orientation of M is given by the sign of a . It follows that $N(M) = 1/a$. We can now calculate Q_M :

$$Q_M(x, y) = \frac{1}{N(M)} N(x - y\gamma) = ax^2 + bxy + cy^2.$$

This shows that Q_M is an integral, primitive binary quadratic form of discriminant $D = b^2 - 4ac$, which is the discriminant of the multiplier ring of M .

On the other hand, if we chose a different proper basis (α', β') of M then the corresponding form is $Q'_M(x, y) = a'x^2 + b'xy + c'y^2$, where

$$\begin{pmatrix} 2a' & b' \\ b' & 2c' \end{pmatrix} = A \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} A^T.$$

Since the two bases have the same orientation, the matrix A has determinant 1. In particular the two forms are properly equivalent.

If Q is a quadratic form, let $[Q]$ denote its proper equivalence class.

Theorem 3.1. *Let D be a fixed discriminant. Then $[(M, \epsilon)] \mapsto [Q_M]$ defines a bijection between the group of narrow classes of full oriented modules corresponding to the unique order of discriminant D , and the set of proper equivalence classes of primitive quadratic forms of the same discriminant D .*

Proof. It is clear, from the discussion preceding the statement of the theorem, that the map is well defined. In order to prove that the map is bijective, it suffices to give the inverse map. To that end, let $Q(x, y) = ax^2 + bxy + cy^2$ be a primitive quadratic form of discriminant D . Let

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Let $M_Q = \{1, \gamma\}$, and ϵ the sign of a . Then $[Q] \mapsto [(M_Q, \epsilon)]$ is the sought inverse map. The theorem is proved. \square

Remark: If $D < 0$ then $Pic^+(R) = Pic(R) \times \{\pm 1\}$ and the restriction to $Pic(R)$, of the bijection between $Pic^+(R)$ and the set of proper classes of primitive forms of discriminant D , gives us a bijection of $Pic(R)$ and the set of proper classes of positive definite, primitive quadratic forms of discriminant D . Thus the order of $Pic(R)$ is finite, by reduction theory, and it can be effectively computed using reduction theory.

Now assume that (M, ϵ) has a proper basis $(1, \gamma)$ which gives rise to the quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ by the recipe described above. Then $(1, -\bar{\gamma})$ is a proper basis of (\bar{M}, ϵ) and it defines $\bar{Q}(x, y) = ax^2 - bxy + cy^2$. Since (\bar{M}, ϵ) is in the inverse class of (M, ϵ) , it follows that (M, ϵ) is an element of order 2 in $Pic^+(R)$ if and only if Q and \bar{Q} are properly equivalent. If $D < 0$, then positive definite Q which are properly equivalent to \bar{Q} have been classified by symmetries of the topograph. In particular, we have:

Proposition 3.2. *Let $D < 0$ be a fundamental discriminant. Write $D = D_1 \cdots D_t$ as a product of prime fundamental discriminants. Then $Pic(R)_2$, the 2-torsion of $Pic(R)$ has the order 2^{t-1} .*

Exercise: Let R be the quadratic order with discriminant $D < 0$. Determine the order of $Pic(R)$, $Pic(R)_2$ if $D = -39, -55, -84, -120$. Using this information, determine the group $Pic(R)$ in these cases.