

**Mathematics W4043 Algebraic Number Theory**  
**Assignment # 4**

Benjamin Church

*Worked With Matthew Lerner-Brecher*

December 17, 2017

1. Let  $q_1(X, Y) = q_1(Xe_1 + Ye_2) = X^2 + 15Y^2$  and  $q_2(X, Y) = 3X^2 + 5Y^2$ . Now,

$$b_{ij}^{(1)} = B_1(e_i, e_j) = q_1(e_i + e_j) - q_1(e_i) - q_1(e_j)$$

Thus,

$$B^{(1)} = \begin{pmatrix} b_{11}^{(1)} & b_{12}^{(1)} \\ b_{21}^{(1)} & b_{22}^{(1)} \end{pmatrix} = \begin{pmatrix} 4 - 1 - 1 & 16 - 1 - 15 \\ 16 - 15 - 1 & 60 - 15 - 15 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 30 \end{pmatrix}$$

Thus, the discriminant,  $\Delta_1 = -\det B^{(1)} = -(2 \cdot 30) = -60$ . Next,

$$b_{ij}^{(2)} = B_2(e_i, e_j) = q_2(e_i + e_j) - q_2(e_i) - q_2(e_j)$$

Thus,

$$B^{(2)} = \begin{pmatrix} b_{11}^{(2)} & b_{12}^{(2)} \\ b_{21}^{(2)} & b_{22}^{(2)} \end{pmatrix} = \begin{pmatrix} 12 - 3 - 3 & 8 - 3 - 5 \\ 8 - 5 - 3 & 20 - 5 - 5 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 10 \end{pmatrix}$$

Thus, the discriminant,  $\Delta_2 = -\det B^{(2)} = -60$ . However, suppose that there existed  $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$  s.t. that  $q_1$  factors as  $q_2 \circ f = q_1$ . Then  $q_1(1, 0) = 1$  so  $q_2 \circ f(1, 0) = 1$  but  $f(1, 0) \in \mathbb{Z}^2$  and on  $\mathbb{Z}^2$  the form  $3X^2 + 5Y^2 \neq 1$  so the desired  $f$  cannot exist.

2. Let  $K = \mathbb{Q}(\sqrt{-d})$  with square-free  $d \in \mathbb{Z}^+$  and  $q(x) = N_{\mathbb{Q}}^K(x)$ .

- (a) If  $d \equiv 1, 2 \pmod{4}$  then  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$  so  $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-d}$  thus,  $\{1, \sqrt{-d}\}$  is a  $\mathbb{Z}$  basis of  $\mathcal{O}_K$  as a  $\mathbb{Z}$ -module of rank 2. Then,

$$b_{ij} = B(e_i, e_j) = q(e_i + e_j) - q(e_i) - q(e_j) = N_{\mathbb{Q}}^K(e_i + e_j) - N_{\mathbb{Q}}^K(e_i) - N_{\mathbb{Q}}^K(e_j)$$

Thus,

$$\begin{aligned} B &= \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} q(1+1) - q(1) - q(1) & q(1+\sqrt{-d}) - q(1) - q(\sqrt{-d}) \\ q(\sqrt{-d}+1) - q(\sqrt{-d}) - q(1) & q(\sqrt{-d}+\sqrt{-d}) - q(\sqrt{-d}) - q(\sqrt{-d}) \end{pmatrix} \\ &= \begin{pmatrix} 4 - 1 - 1 & 1 + d - 1 - d \\ 1 + d - d - 1 & 4d - d - d \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} \end{aligned}$$

Thus, the discriminant,  $\Delta_q = -\det B = -4d$ .

If  $d \equiv 3 \pmod{4}$  then  $\mathcal{O}_K = \mathbb{Z} \left[ \frac{1+\sqrt{-d}}{2} \right]$  so  $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \frac{1+\sqrt{-d}}{2}$  thus,  $\left\{ 1, \frac{1+\sqrt{-d}}{2} \right\}$  is a  $\mathbb{Z}$  basis of  $\mathcal{O}_K$  as a  $\mathbb{Z}$ -module of rank 2. Then,

$$b_{ij} = B(e_i, e_j) = q(e_i + e_j) - q(e_i) - q(e_j) = N_{\mathbb{Q}}^K(e_i + e_j) - N_{\mathbb{Q}}^K(e_i) - N_{\mathbb{Q}}^K(e_j)$$

Thus,

$$\begin{aligned} B &= \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{11} \end{pmatrix} \\ &= \begin{pmatrix} q(1+1) - q(1) - q(1) & q\left(1 + \frac{1+\sqrt{-d}}{2}\right) - q(1) - q\left(\frac{1+\sqrt{-d}}{2}\right) \\ q\left(\frac{1+\sqrt{-d}}{2} + 1\right) - q\left(\frac{1+\sqrt{-d}}{2}\right) - q(1) & q\left(\frac{1+\sqrt{-d}}{2} + \frac{1+\sqrt{-d}}{2}\right) - q\left(\frac{1+\sqrt{-d}}{2}\right) - q\left(\frac{1+\sqrt{-d}}{2}\right) \end{pmatrix} \\ &= \begin{pmatrix} 4 - 1 - 1 & \frac{9}{4} + \frac{d}{4} - 1 - \left(\frac{1}{4} + \frac{d}{4}\right) \\ \frac{9}{4} + \frac{d}{4} - \left(\frac{1}{4} + \frac{d}{4}\right) - 1 & 1 + d - \left(\frac{1}{4} + \frac{d}{4}\right) - \left(\frac{1}{4} + \frac{d}{4}\right) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix} \end{aligned}$$

Thus, the discriminant,  $\Delta_q = -\det B = -d$ . Therefore, in either case,  $\Delta_q = \Delta_d$ . Both quadratic forms are positive definite due to the positive definiteness of the complex conjugate norm on  $\mathbb{C}$  i.e.  $z \neq 0 \implies z\bar{z} > 0$  so  $x \neq 0 \implies q(x) = N_{\mathbb{Q}}^K(x) = x\bar{x} > 0$ . These are equivalent because the only non identity Galois conjugate in an order two complex field extension is complex conjugation and thus  $N_{\mathbb{Q}}^K(x) = x\sigma(x) = x\bar{x}$ .

- (b)  $K$  is a complex field extension of  $\mathbb{Q}$  thus the element  $\sigma : x \mapsto \bar{x}$  is a non-identity automorphism in  $\text{Gal}(K/\mathbb{Q})$ . Since the order of  $K/\mathbb{Q} = 2$  this must be the only non-identity Galois conjugate. Now for  $\tau$  ranging over all  $G = \text{Gal}(K/\mathbb{Q})$

$$q(x) = N_{\mathbb{Q}}^K(x) = \prod_{\tau \in G} \tau(x) = \text{id}(x)\sigma(x) = x\sigma(x)$$

Thus,

$$\begin{aligned} B_q(x, y) &= q(x+y) - q(x) - q(y) = (x+y)\sigma(x+y) - x\sigma(x) - y\sigma(y) \\ &= x\sigma(x) + x\sigma(y) + y\sigma(x) + y\sigma(y) - x\sigma(x) - y\sigma(y) \\ &= x\sigma(y) + y\sigma(x) = x\sigma(y) + \sigma^2(y)\sigma(x) = x\sigma(y) + \sigma(x\sigma(x)) \\ &= \text{Tr}_{\mathbb{Q}}^K(x\sigma(y)) \end{aligned}$$

in which i have used the fact that  $\sigma^2 = \text{id}$  which holds because the order of the Galois group is 2.

- (c) Let  $I \subset \mathcal{O}_K$  be an ideal and define  $q_I : I \rightarrow \mathbb{Q}$  by  $q_I(x) = N_{\mathbb{Q}}^K(x)/N(I)$ . First, for any  $\alpha \in I$  by closure of ideals,  $(\alpha) \subset I$  thus by Dedekind prime factorization, there exists an ideal  $J \subset \mathcal{O}_K$  such that  $(\alpha) = IJ$  so in particular,  $N_{\mathbb{Q}}^K(\alpha) = N((\alpha)) = N(I)N(J)$  so  $N(I) \mid N_{\mathbb{Q}}^K(\alpha)$ . Thus,  $q_I(\alpha) = N_{\mathbb{Q}}^K(\alpha)/N(I) \in \mathbb{Z}$ . Since,  $N_{\mathbb{Q}}^K(\alpha)$  is a norm on  $I$  then because  $N(I)$  is constant,  $q_I(\alpha) = N_{\mathbb{Q}}^K(\alpha)/N(I) \in \mathbb{Z}$  satisfies all the norm axioms and by above has its image inside  $\mathbb{Z}$ . Thus,  $q_I$  is a perfectly good norm and  $I$  is a  $\mathbb{Z}$ -module of free rank 2 because  $[K : \mathbb{Q}] = 2$  implies that  $\mathcal{O}_K$  is a  $\mathbb{Z}$ -module of free rank 2 and  $I$  is a submodule of finite type. Thus,  $(I, q_I)$  is a quadratic space.
- (d) Since  $[K : \mathbb{Q}] = 2$  then  $\mathcal{O}_K$  is a  $\mathbb{Z}$ -module of free rank 2 so  $\mathcal{O}_K = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$  and any ideal  $I \subset \mathcal{O}_K$  is also a  $\mathbb{Z}$ -module of free rank 2 expressed as  $I = \mathbb{Z}e_1c_1 \oplus \mathbb{Z}e_2c_2$  for  $c_1, c_2 \in \mathbb{Z}$ .

Then  $\mathcal{O}_K/I \cong \mathbb{Z}/c_1\mathbb{Z} \times \mathbb{Z}/c_2\mathbb{Z}$  so  $N(I) = [\mathcal{O}_K : I] = [\mathbb{Z} : c_1\mathbb{Z}][\mathbb{Z} : c_2\mathbb{Z}] = c_1c_2$ . Now we calculate the matrix associated with the bilinear form,

$$\begin{aligned} b_{ij} &= B_I(e_i c_i, e_j c_j) = q(e_i c_i + e_j c_j) - q(e_i c_i) - q(e_j c_j) \\ &= (N_{\mathbb{Q}}^K(e_i c_i + e_j c_j) - N_{\mathbb{Q}}^K(e_i c_i) - N_{\mathbb{Q}}^K(e_j c_j))/N(I) \\ &= B_K(e_i c_i, e_j c_j)/N(I) = (e_i c_i \sigma(e_j c_j) + e_j c_j \sigma(e_i c_i))/N(I) \end{aligned}$$

But integers are fixed under every automorphism thus,

$$b_{ij}^I = B_I(e_i c_i, e_j c_j) = (e_i \sigma(e_j) + e_j \sigma(e_i))c_i c_j / N(I) = B_K(e_i, e_j) c_i c_j / N(I) = b_{ij} c_i c_j / N(I)$$

Thus,

$$B_I = \begin{pmatrix} b_{11}^I & b_{12}^I \\ b_{21}^I & b_{11}^I \end{pmatrix} = \frac{1}{N(I)} \begin{pmatrix} b_{11}c_1^2 & b_{12}c_1c_2 \\ b_{21}c_2c_1 & b_{22}c_2^2 \end{pmatrix}$$

Thus, the discriminant,

$$\begin{aligned} \Delta_I &= -\det B^I = -(b_{11}b_{22}(c_1c_2)^2 - b_{12}b_{21}(c_1c_2)^2)/N(I)^2 \\ &= -(b_{11}b_{22} - b_{12}b_{21})(c_1c_2)^2/N(I)^2 = -\det B = \Delta_d \end{aligned}$$

because  $N(I) = c_1c_2$  and from before,  $\Delta_d = -\det B = -(b_{11}b_{22} - b_{12}b_{21})$ .

3. Let  $D(x_1, \dots, x_n) = \det \text{Tr}(x_1, x_2)$ .

(a)  $\text{Tr}(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j)$ . Now define  $A_{ki} = \sigma_k(x_i)$  then,

$$\sum_{k=1}^n \sigma_k(x_i x_j) = \sum_{k=1}^n A_{ki} A_{kj} = \sum_{k=1}^n (A^\top)_{ik} A_{kj} = (A^\top A)_{ij}$$

Thus,

$$D(x_1, \dots, x_n) = \det \text{Tr}(x_1, x_2) = \det (A^\top A) = (\det A)^2 = (\det \sigma_i(x_j))^2$$

(b) Let  $y_i = \sum_{j=1}^n A_{ij} x_j$  with  $A_{ij} \in \mathbb{Q}$ . Now,

$$\begin{aligned} D(y_1, \dots, y_n) &= (\det \sigma_i(y_j))^2 = \left( \det \sigma_i \left( \sum_{k=1}^n A_{jk} x_k \right) \right)^2 = \left( \det \left( \sum_{k=1}^n \sigma_i(x_k) (A^\top)_{kj} \right) \right)^2 \\ &= (\det A)^2 (\det \sigma_i(x_j))^2 = (\det A)^2 D(x_1, \dots, x_n) \end{aligned}$$

(c) Let  $K = \mathbb{Q}(\alpha)$  and  $f$  be the minimal polynomial of  $\alpha$ . Now,

$$f(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) \dots (x - \sigma_n(\alpha)) = \prod_{i=1}^n (x - \sigma_i(\alpha))$$

because the embeddings permute the roots of  $f$ . Thus,

$$f'(x) = \sum_{k=1}^n \prod_{j \neq k} (x - \sigma_j(\alpha))$$

Plugging in a root,

$$f'(\sigma_i(\alpha)) = \sum_{k=1}^n \prod_{j \neq k}^n (\sigma_i(\alpha) - \sigma_j(\alpha)) = \prod_{j \neq i}^n (\sigma_i(\alpha) - \sigma_j(\alpha))$$

Now consider the norm,

$$N_{\mathbb{Q}}^K(f'(\alpha)) = \prod_{i=1}^n \sigma_i(f'(\alpha)) = \prod_{i=1}^n f'(\sigma_i(\alpha)) = \prod_{i=1}^n \prod_{j \neq i}^n (\sigma_i(\alpha) - \sigma_j(\alpha))$$

which holds because each  $\sigma_i$  is an automorphism. This product ranges twice over all pairs but in the opposite orders. Therefore, this product is equal to the square of the product over all pairs multiplied by  $n(n-1)/2$  (the number of pairs) minus signs from swapping the orders of terms i.e.

$$N_{\mathbb{Q}}^K(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \left[ \prod_{i > j}^n (\sigma_i(\alpha) - \sigma_j(\alpha)) \right]^2$$

By Vandermonde's determinant formula,

$$\prod_{i > j}^n (\sigma_i(\alpha) - \sigma_j(\alpha)) = \det \sigma_i(\alpha)^{j-1} = \det \sigma_i(\alpha^{j-1})$$

Thus,

$$\left[ \prod_{i > j}^n (\sigma_i(\alpha) - \sigma_j(\alpha)) \right]^2 = (\det \sigma_i(\alpha^{j-1}))^2 = D(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$$

Therefore,

$$D(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbb{Q}}^K(f'(\alpha))$$

However, the  $f'(\alpha) \neq 0$  because  $f$  is the minimal polynomial of  $\alpha$  and thus does not have a double root at  $\alpha$ . Therefore,  $N_{\mathbb{Q}}^K(f'(\alpha)) \neq 0$  and thus,  $D(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) \neq 0$ . A set of  $n$  elements  $\{x_1, \dots, x_n\}$  forms a basis if and only if it is related to some basis by an invertible matrix. In particular,  $\{x_1, \dots, x_n\}$  is a basis iff the matrix  $A$  such that  $x_i = \sum_{j=1}^n A_{ij} \alpha^{j-1}$  is invertible. In this case,

$$D(x_1, \dots, x_n) = (\det A)^2 D(1, \alpha, \dots, \alpha^{n-1})$$

Because  $D(1, \alpha, \dots, \alpha^{n-1}) \neq 0$ , we have that,

$$D(x_1, \dots, x_n) = 0 \iff \det A = 0 \iff A \text{ is invertible} \iff \{x_1, \dots, x_n\} \text{ is a basis}$$

Because a bilinear form is degenerate if and only if its associated matrix has zero determinant, we conclude that,

$$\text{Tr}(xy) \text{ is degenerate} \iff \det \text{Tr}(x_i x_j) = D(x_1, \dots, x_n) = 0 \iff \{x_1, \dots, x_n\} \text{ is a basis}$$

4. Let  $\{v_1, \dots, v_n\}$  be a basis of  $\mathbb{R}^n$  then define:

$$G = \left\{ \sum_{i=1}^n z_i v_i \mid z_i \in \mathbb{Z} \right\}$$

and

$$D = \left\{ \sum_{i=1}^n d_i v_i \mid d_i \in [0, 1) \right\}$$

(a) Let  $v \in \mathbb{R}^n$  then because  $\{v_1, \dots, v_n\}$  is a basis, there is a decomposition with  $c_i \in \mathbb{R}$ ,

$$v = c_1 v_1 + \dots + c_n v_n$$

Now take  $d_i = \lfloor c_i \rfloor$  and  $z_i = c_i - \lfloor c_i \rfloor$ . We have  $z_i + d_i = c_i - \lfloor c_i \rfloor + \lfloor c_i \rfloor = c_i$  also,  $z_i \in \mathbb{Z}$  and  $d_i = \lfloor c_i \rfloor \in [0, 1)$ . Now take,

$$g = \sum_{i=1}^n z_i v_i \in G \quad \text{and} \quad d = \sum_{i=1}^n d_i v_i \in D$$

And therefore,

$$g + d = \sum_{i=1}^n (z_i + d_i) v_i = \sum_{i=1}^n c_i v_i = v$$

Suppose there were another decomposition,  $g' + d' = v$  with

$$g' = \sum_{i=1}^n z'_i v_i \in G \quad \text{and} \quad d' = \sum_{i=1}^n d'_i v_i \in D$$

and then,

$$g + d = \sum_{i=1}^n (z'_i + d'_i) v_i = v$$

but  $\{v_1, \dots, v_n\}$  is a basis so the decomposition is unique. Thus,  $z'_i + d'_i = z_i + d_i$  so  $z'_i - z_i = d_i - d'_i \in \mathbb{Z}$  but  $z_i, z'_i \in [0, 1)$  so  $z'_i = z_i$  and thus  $d_i = d'_i$  so the decomposition in  $G$  and  $D$  is indeed unique.

(b) Using the notation  $B_\delta(x) = \{v \in \mathbb{R}^n \mid |v - x| < \delta\}$ . Now,  $G$  is a discrete set because around each  $g \in G$  the ball  $B_{\frac{1}{2}}(g)$  contains no other points of  $G$ . Also,  $D$  is a bounded set i.e.  $D \subset B_R(0)$  for  $R = |v_1| + \dots + |v_n|$ . Define the set

$$H = \{h \in G \mid B_r(0) \cap D_h \neq \emptyset\}$$

Thus,  $D_h \subset B_R(h)$  so if  $B_r(0) \cap D_h \neq \emptyset$  then  $\exists x \in B_r(0) \cap D_h$  so  $|h| < |x| + |h - x| < r + R$  because  $x$  is in both balls. Thus, if  $h \in H$  then  $|h| < r + R = \delta$  so  $H \subset B_\delta(0) \subset \overline{B_\delta(0)}$ . The closure of this ball is compact by Heine-Borrel. Furthermore,  $H \subset G$  by construction so  $H \subset G \cap \overline{B_\delta(0)}$ . However,  $G$  is discrete and  $\overline{B_\delta(0)}$  is compact so their intersection is finite. Thus,  $H$  is finite.