Algebra III
Home Assignment 4

Subhadip Chowdhury

Problem 11

■ We will denote the quadratic form $q(x, y) = ax^2 + bxy + cy^2$ by the ordered tuple (a, b, c). We are given that d is a negative squarefree integer congruent to $1 \mod 4$. Since $K = \mathbb{Q}[\sqrt{d}]$, we have

$$\mathcal{O}_K = R = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$$

Let us define

$$\mathcal{F}_d = \text{The set of integral quadratic forms of discriminant } d \text{ modulo } SL_2(\mathbb{Z})\text{-equivalence}$$

and let $\mathcal{F}_d^+$ denote those elements of $\mathcal{F}_d$ represented by a positive definite quadratic form(i.e. a form (a, b, c) with $a > 0$, since $d < 0$).

Define the function $\Phi : \mathcal{F}_d \to Cl(R)$ by

$$\Phi(a, b, c) = a\mathbb{Z} + \frac{b - \sqrt{d}}{2}\mathbb{Z}$$

and define $\Psi : Cl(R) \to \mathcal{F}_d$ by

$$\Psi(\mathfrak{a}) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}$$

where $\{\alpha, \beta\}$ is a $\mathbb{Z}-$basis of $\mathfrak{a}$ such that

$$\frac{\alpha\beta' - \beta\alpha'}{\sqrt{d}} > 0 \qquad (\star)$$

Here α' denotes the Galois conjugate of α in K.

We claim that Φ and Ψ are well defined and induce bijections from $\mathcal{F}_d^+$ to $Cl(R)$.

♦ **To check Φ is well defined:** First of all we check that if $b^2 - 4ac = d \equiv 1 \mod 4$, then b is odd, so

$$\frac{b-\sqrt{d}}{2} \in \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z} = \mathcal{O}_K$$

Now if $\begin{pmatrix} A & B \\ U & V \end{pmatrix}$, an element of $SL_2(\mathbb{Z})$ acts on (a,b,c) then the quantity $\tau = \frac{-b+\sqrt{d}}{2a}$ becomes

$$\tau' = \frac{V\tau - B}{-U\tau + A}$$

and a becomes

$$a' = aN(-U\tau + A)$$

Now in $Cl(R)$,

$$a'(\mathbb{Z} + (-\tau')\mathbb{Z}) = \frac{aN(-U\tau + A)}{-U\tau + A}(\mathbb{Z} + (-\tau)\mathbb{Z}) = a(\mathbb{Z} + (-\tau)\mathbb{Z})$$

since $\frac{aN(-U\tau+A)}{-U\tau+A} \in K^\times$. Thus Φ is well defined.

♦ **To check Ψ is well defined:** Say a basis $\{\alpha, \beta\}$ of I, an ideal of R is *correctly ordered* if $(\star)$ is satisfied. We prove the following lemma:

Lemma 1: Any two *correctly ordered* bases of an ideal I are equivalent by an element in $SL_2(\mathbb{Z})$, and conversely.

Proof: Suppose $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ are two *correctly ordered* bases for an ideal I. Because these are two different basis for the same free $\mathbb{Z}$-module, there are $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = A \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

and $\det(A) = \pm 1$. Since $a, b, c, d \in \mathbb{Z}$ and the conjugation automorphism fixes $\mathbb{Z}$, we have

$$\begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix}$$

Taking determinants we have

$$\alpha\beta' - \beta\alpha' = \det(A)(\gamma\delta' - \delta\gamma') \tag{$\dagger$}$$

Since $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ are correctly oriented, we must have $\det(A) = +1$. So $A \in SL_2(\mathbb{Z})$.

Conversely, if $A \in SL_2(\mathbb{Z})$ and $\{\gamma, \delta\}$ is a correctly oriented basis then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix} = \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}$$

and by $(\dagger)$, $\{\alpha, \beta\}$ is also correctly oriented. ■

Lemma 2: Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ and Let $\{\alpha, \beta\}$ be a basis of $\mathfrak{a}$. Since $d \equiv 1 \mod 4$, the absolute discriminant of K is d. Then

$$\det \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}^2 = dN(\mathfrak{a})^2$$

Proof: Let $\{\gamma, \delta\}$ be a basis for $\mathcal{O}_K$. Since α and β can be written as a $\mathbb{Z}-$linear combination of γ and δ there is a 2×2 matrix A such that

$$A \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

We have

$$\det \begin{pmatrix} \alpha & \alpha' \\ \beta & \beta' \end{pmatrix}^2 = \det \left(A \begin{pmatrix} \gamma & \gamma' \\ \delta & \delta' \end{pmatrix} \right)^2 = \det(A)^2 d = N(\mathfrak{a})^2 . d$$

■

We next prove that $\Psi(\mathfrak{a}) \in \mathcal{F}_d^+$. Let $\{\alpha, \beta\}$ be a correctly ordered basis of $\mathfrak{a}$ and

$$\begin{aligned} N(\alpha x + \beta y) &= (\alpha x + \beta y)(\alpha' x + \beta' y) \\ &= \alpha\alpha' x^2 + (\alpha\beta' + \beta\alpha')xy + \beta\beta' y^2 \\ &= Ax^2 + Bxy + Cy^2 \end{aligned}$$

The coefficients A, B, C are integers since they are norms and traces. We claim that in fact $A, B, C \in (N(\mathfrak{a}))$. Note that if $\alpha \in \mathfrak{a}$, then $N(\alpha) \in (N(\mathfrak{a}))$. Thus $A = N(\alpha) \in (N(\mathfrak{a}))$. Similarly $C = N(\beta) \in (N(\mathfrak{a}))$ and $(N(\alpha+\beta) - N(\alpha-\beta)) \in (N(\mathfrak{a})) \Rightarrow B \in (N(\mathfrak{a}))$. Let $A = aN(\mathfrak{a}), B = bN(\mathfrak{a}), C = cN(\mathfrak{a})$. Since $A, N(\mathfrak{a})$ are both in $\mathbb{Z}$ and $R = \mathcal{O}_K$, we see that $a \in \mathbb{Z}$. Likewise $b, c \in \mathbb{Z}$. Thus $\Psi(\mathfrak{a}) = ax^2 + bxy + cz^2$ has coefficients in $\mathbb{Z}$. Now

$$b^2 - 4ac = \frac{B^2 - 4AC}{N(\mathfrak{a})^2} = \frac{(\alpha\beta' - \beta\alpha')^2}{N(\mathfrak{a})^2} = d$$

Thus $\Psi(\mathfrak{a}) \in \mathcal{F}_d^+$.

Note that by lemma 1, Ψ is independent of the choice of basis for $\mathfrak{a}$ Choosing a different basis amounts to changing the basis from $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ to $\begin{pmatrix} \gamma \\ \delta \end{pmatrix}$ obtained by multiplying $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ by an element $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $SL_2(\mathbb{Z})$; so that

$$N((a\alpha + b\beta)x + (c\alpha + d\beta)y) = N(\alpha(ax + cy) + \beta(bx + dy)$$

and hence the new quadratic form is a $SL_2(\mathbb{Z})$ conjugate of the old quadratic form. So in $\mathcal{F}_d^+$, they are equal.

Thus Ψ does not depend on the choice of basis. Also if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same equivalence class. Then there exists $\mu, \lambda \in \mathcal{O}_K$ such that

$$\mu\mathfrak{a} = \lambda\mathfrak{b} \text{ and } N(\mu\lambda) > 0$$

Then $\{\gamma, \delta\}$ forms a basis of $\mathfrak{b}$ where $\mu\alpha = \lambda\gamma$ and $\mu\beta = \lambda\delta$. Also $\mu\mu' N(\mathfrak{a}) = N(\mu\mathfrak{a}) = N(\lambda\mathfrak{b}) = \lambda\lambda' N(\mathfrak{b})$. Hence the ratio of $N(\gamma x + \delta y)$ and $N(\mathfrak{b})$ is equal to $\Psi(\mathfrak{a})$. Thus Ψ is constant on the equivalence class of $\mathfrak{a}$. Thus we have proved that Ψ is well defined.

♦ **To show Φ and Ψ are inverse maps:** Suppose we have a quadratic form (a,b,c) with $b^2-4ac=d$. We want to show that

$$\Psi\circ\Phi(a,b,c)=(a,b,c) \text{ in } \mathcal{F}_d^+$$

Now it is easy to check that $\{a,\frac{b-\sqrt{d}}{2}\}$ is correctly ordered if $a>0$. Then by definition,

$$\begin{aligned}\Psi\left(a\mathbb{Z}+\frac{b-\sqrt{d}}{2}\mathbb{Z}\right)&=\frac{N(ax+\frac{b-\sqrt{d}}{2}y)}{N\left(a\mathbb{Z}+\frac{b-\sqrt{d}}{2}\mathbb{Z}\right)}\\&=\frac{a^2x^2+abxy+\frac{b^2-d}{4}y^2}{(a\sqrt{d})/\sqrt{d}} \qquad \text{[We used Lemma 2]}\\&=ax^2+bxy+cy^2\end{aligned}$$

Thus

$$\Psi\circ\Phi=Id_{\mathcal{F}_d^+}$$

Next suppose we have a fractional ideal $\mathfrak{a}$. Then if $\{\alpha,\beta\}$ is a correctly ordered basis for $\mathfrak{a}$ then as shown above $\Psi(\mathfrak{a})=ax^2+bxy+cy^2$ with $b^2-4ac=d$ and $a=A/N(\mathfrak{a})$ etc. So

$$\begin{aligned}\Phi(a,b,c)&=\frac{\alpha\alpha'}{N(\mathfrak{a})}\mathbb{Z}+\frac{(\alpha\beta'+\beta\alpha')/N(\mathfrak{a})-\sqrt{d}}{2}\mathbb{Z}\\&=\sqrt{d}\frac{\alpha\alpha'}{\alpha\beta'-\beta\alpha'}\mathbb{Z}+\sqrt{d}\frac{\frac{\alpha\beta'+\beta\alpha'}{\alpha\beta'-\beta\alpha'}-1}{2}\mathbb{Z}\\&=\sqrt{d}\frac{\alpha\alpha'}{\alpha\beta'-\beta\alpha'}\mathbb{Z}+\sqrt{d}\frac{\beta\alpha'}{\alpha\beta'-\beta\alpha'}\mathbb{Z}\end{aligned}$$

Hence

$$(\alpha\beta'-\beta\alpha')\Phi(a,b,c)=(\sqrt{d}\alpha')\mathfrak{a}$$

Hence we can find suitable $\mu,\lambda\in\mathcal{O}_K$ such that $\mu\Phi(a,b,c)=\lambda\mathfrak{a}$. So in $Cl(R)$, $\Phi(a,b,c)=\mathfrak{a}$ implying

$$\Phi\circ\Psi=Id_{Cl(R)}$$

Thus we have proved that Φ and Ψ are well defined and induce bijections from $\mathcal{F}_d^+$ to $Cl(R)$.

■■ We have to prove two things. First, that every $SL_2(\mathbb{Z})-$equivalence class of positive definite quadratic form of discriminant $d<0$ contains at least one reduced form, and second that this reduced form is the only one in the equivalence class.

We first prove that there is a reduced form in every class. Let $\mathcal{C}$ be an equivalence class of positive definite quadratic forms of discriminant d. Let (a,b,c) be an element of $\mathcal{C}$ such that a is minimal (amongst elements of $\mathcal{C}$). Note that for any such form we have $c\geq a$, since (a,b,c) is equivalent to $(c,-b,a)$ using the matrix $\begin{pmatrix}0&-1\\1&0\end{pmatrix}\in SL_2(\mathbb{Z})$. Applying the element $\begin{pmatrix}1&k\\0&1\end{pmatrix}\in SL_2(\mathbb{Z})$ to (a,b,c) for a suitably chosen integer k (precisely, $k=\lfloor(a-b)/2a\rfloor$) results in a form (a',b',c') with $a'=a$ and $b'\in(-a',a']$. Since $a'=a$ is minimal, we have just as above that $a'\leq c'$, hence (a',b',c') is reduced except in the case when $a'=c'$ and $b'<0$. In that case, changing (a',b',c') to $(c'',b'',a'')=(c',-b',a')$ results in an equivalent form with $b''>0$, so that (c'',b'',a'') is reduced.

Next suppose (a, b, c) is a reduced form. We will now establish that (a, b, c) is the only reduced form in its equivalence class. First, we check that a is minimal amongst all forms equivalent to (a, b, c). Indeed, every other a' has the form $a' = ap^2 + bpr + cr^2$ with $(p, r) = 1$. The identities

$$ap^2 + bpr + cr^2 = ap^2\left(1 + \frac{br}{ap}\right) = ap^2 + cr^2\left(1 + \frac{bp}{cr}\right)$$

then impll our claim since $|b| \leq a \leq c$(using first identity if $r/p < 1$ and the second otherwise). Thus any other reduced form (a', b', c') equivalent to (a, b, c) ahs $a = a'$. But the same identity implies that the only forms equivalent to (a, b, c) with $a' = a$ are obtained by applying a transformation of the form $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (corresponding to $p = 1, r = 0$). Thus $b' = b + 2ak$ for some k. Since $a = a'$, we have $b, b' \in (-a, a]$, so $k = 0$. Finally

$$c' = \frac{(b')^2 - d}{4a} = \frac{b^2 - d}{4a} = c$$

So $(a, b, c) = (a', b', c')$.

■■■ The class number $h_d = Cl(R)$ for $d \equiv 1 \mod 4$ and $d < 0$ is equal to the number of equivalence classes of positive definite quadratic forms of discriminant d which is same as the number of reduced positive definite quadratic form of discriminant d. Note that if a form (a, b, c) is reduced then $0 \leq |b| \leq a \leq c$.Then $d = b^2 - 4ac$ implies

$$b^2 \leq a^2 \leq ac \Rightarrow d \leq -3ac \Rightarrow 3ac \leq -d$$

- For $d = -3$, $3ac \leq 3 \Rightarrow ac \leq 1 \Rightarrow ac = 1 = a = c \Rightarrow b^2 = 1 \Rightarrow b = 1$ since $a = c \Rightarrow b \geq 0$. Thus there is only one possibility implying $h_d = 1$.
- For $d = -7$, $3ac \leq 7 \Rightarrow ac \leq 2 \Rightarrow ac = 1, 2$. If $ac = 1$, then $a = c = 1$ and $b^2 = -3$, not possible. Hence $ac = 2$. Then $b^2 = 1 \Rightarrow b = 1$. Thus $|b| \leq a \leq c \Rightarrow (a, b, c) = (1, 1, 2)$. So again $h_d = 1$.
- For $d = -11$, $3ac \leq 11 \Rightarrow ac = 1, 2, 3$. If $ac = 1, 2$, $b^2 = -7, -3$, not possible. If $ac = 3$, $b^2 = 1 \Rightarrow b = 1 \Rightarrow (a, b, c) = (1, 1, 3)$. So $h_d = 1$.
- For $d = -15$, $3ac \leq 15 \Rightarrow ac = 1, 2, 3, 4, 5$. If $ac = 1, 2, 3$ we get $b^2 < 0$, not possible. If $ac = 4$, $b^2 = 1 \Rightarrow (a, b, c) = (1, 1, 4)$ or $(2, 1, 2)$. If $ac = 5$, $b^2 = 5$, not possible. Thus $h_d = 2$.
- For $d = -19$, $3ac \leq 19 \Rightarrow ac = 1, 2, 3, 4, 5, 6$. If $ac = 1, 2, 3, 4$, we have $b^2 < 0$. For $ac = 5$, $b^2 = 1 \Rightarrow (a, b, c) = (1, 1, 5)$. For $ac = 6$, $b^2 = 5$, not possible. thus $h_d = 1$.

Problem 12

For a commutative ring A and a ring extension B of A which is a finite free A-module:

$$B = Av_1 \oplus Av_2 \oplus \ldots \oplus Av_n$$

We write

$$\text{disc}_A(B) = \text{disc}_A(v_1, \ldots, v_n) = \det(\text{Tr}_{B/A}(v_iv_j)) \in A$$

In particular, the absolute discriminant of L is then $\text{disc}_{\mathbb{Z}}(\mathcal{O}_L)$. Note that given a number field L, there is a place ν of L over p which is ramified is equivalent to the fact that the prime ideal factorization

$$(p) = p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \ldots \tag{1}$$

has some e_i greater than 1. Now by Chinese remainder theorem and by (1),

$$\mathcal{O}_L/(p) \cong \mathcal{O}_L/\mathfrak{p}_1^{e_1} \times \ldots \times \mathcal{O}_L/\mathfrak{p}_g^{e_g} \tag{2}$$

If some e_i is greater than 1, then the quotient ring $\mathcal{O}_L/\mathfrak{p}_i^{e_i}$ has a nonzero nilpotent element, so the product ring (2) has a nonzero nilpotent element. If each e_i equals 1, then $\mathcal{O}_L/(p)$ is a product of finite fields, and hence has no nonzero nilpotent elements. Thus p ramifies in L iff $\mathcal{O}_L/(p)$ has a nonzero nilpotent element.

Let degree of L over $\mathbb{Q}$ be n. Then the ring $\mathcal{O}_L$ is a free rank-n free $\mathbb{Z}$-module, say

$$\mathcal{O}_L = \bigoplus_{i=1}^{n} \mathbb{Z}\omega_i$$

Reducing both sides modulo p,

$$\mathcal{O}_L/(p) = \bigoplus_{i=1}^{n} (\mathbb{Z}/p\mathbb{Z})\overline{\omega}_i$$

where $\overline{\omega}_i = \omega_i \mod p$ So $\mathcal{O}_L/(p)$ is a $\zeta/p\mathbb{Z}$ vector space of dimension n. We prove the following lemma:

Lemma 1: Choosing bases appropriately for $\mathcal{O}_L$ and $\mathcal{O}_L/(p)$

$$\text{disc}_{\mathbb{Z}}(\mathcal{O}_L) \mod p = \text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/(p))$$

Proof: Pick a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ for $\mathcal{O}_L$. Then writing $\overline{\omega}_i = \omega_i \mod p$, we get that $\overline{\omega}_i$ forms a $\mathbb{Z}/p\mathbb{Z}$ basis of $\mathcal{O}_L/(p)$. So the multiplication matrix $[m_x]$ for any $x \in \mathcal{O}_L$ w.r.t. $\{\omega_i\}$ reduces modulo p to the multiplication matrix $[m_{\overline{x}}]$ for $\overline{x}$ on $\mathcal{O}_k/(p)$ w.r.t. $\{\overline{\omega}_i\}$. Therefore,

$$Tr_{(\mathcal{O}_L/(p))/(\mathbb{Z}/p\mathbb{Z})}(\overline{\omega_i\omega_j}) = Tr(m_{\overline{\omega_i\omega_j}}) = Tr(m_{\omega_i\omega_j}) \mod p = Tr_{\mathcal{O}_L/Z}(\omega_i\omega_j) \mod p$$

Taking determinants on both sides gives our result. ■

Thus by the lemma we have, $p|\text{disc}_{\mathbb{Z}}(\mathcal{O}_L)$ if and only if $\text{disc}_{\mathbb{Z}}(\mathcal{O}_L) \equiv 0 \mod p$ if and only if $\text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/(p)) = \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$.

In (2), each factor $\mathcal{O}_L/\mathfrak{p}_i^{e_i}$ is a $\mathbb{Z}/p\mathbb{Z}$ vector space since $p \in \mathfrak{p}_i^{e_i}$. So we can write

$$\text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/(p)) = \prod_{i=1}^{g} \text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/\mathfrak{p}_i^{e_i})$$

Therefore we need to show that for any prime p and prime-power ideal $\mathfrak{p}^e$ such that $\mathfrak{p}^e|(p)$ we have

$$\text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/\mathfrak{p}^e) = \overline{0} \in \mathbb{Z}/p\mathbb{Z} \iff e > 1$$

♦ **Suppose** $e > 1$. Then any $x \in \mathfrak{p} - \mathfrak{p}^e$ is a nonzero nilpotent element in $\mathcal{O}_L/\mathfrak{p}^e$. Extend $\overline{x}$ to a $\mathbb{Z}/p\mathbb{Z}$-basis of $\mathcal{O}_L/\mathfrak{p}^e$, say $\{\overline{x} = \overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n\}$. Let us denote $Tr_{(\mathcal{O}_L/\mathfrak{p}^e)/(\mathbb{Z}/p\mathbb{Z})}$ by Tr. The first column of the matrix $[Tr(\overline{x}_i\overline{x}_j)]$ contains the numbers $Tr(\overline{x}_i\overline{x})$. We claim that these traces are all $\overline{0}$. Indeed all the $\overline{x}_i\overline{x}$ are nilpotent. Hence the linear transformation $m_{\overline{x}_i\overline{x}}$ on $\mathcal{O}_L/\mathfrak{p}^e$ is nilpotent. Thus all the eigenvalues are zero. Hence $Tr(\overline{x}_i\overline{x}) = \overline{0}$. Since one column of $[Tr(\overline{x}_i\overline{x}_j)]$ is zero, the determinant is zero as well. Hence $\text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/\mathfrak{p}^e) = \overline{0}$.

♦ **Suppose** $e = 1$. Then $\mathcal{O}_L/\mathfrak{p}^e = \mathcal{O}_L/\mathfrak{p}$ is a finite field of characteristic p. Suppose, on contrary to what we have to prove, $\text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_L/\mathfrak{p}) = \overline{0}$. Note that this condition is independent of the basis. Since $\mathcal{O}_L/\mathfrak{p}$ is a field, this means the function $Tr : \mathcal{O}_L/\mathfrak{p} \to \mathbb{Z}/p\mathbb{Z}$ is identically zero. On the other hand $\mathbb{Z}/p\mathbb{Z}$ is a finite field, hence $\mathcal{O}_L/\mathfrak{p}$ is separable. Let $\#(\mathcal{O}_L/\mathfrak{p}) = p^r$. Then for any element $t \in \mathcal{O}_L/\mathfrak{p}$, the conjugates of t under different embeddings of $\mathcal{O}_L/\mathfrak{p} \cong \mathbb{F}_{p^r}$ in closure of $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ are given by images of t under powers of the Frobenius automorphism. Thus

$$Tr(t) = t + t^p + t^{p^2} + \ldots + t^{p^{r-1}}$$

Since this polynomial has degree less than the size of $\mathcal{O}_L/\mathfrak{p}$, it cannot be identically zero on all of $\mathcal{O}_L/\mathfrak{p}$. Contradiction!!

Problem 13

We will prove that there are only finitely many fields $K/\mathbb{Q}$ of degree n and discriminant d. Note that the discriminant of the field extension $K(\sqrt{-1})/\mathbb{Q}$ differs from the discriminant of $K/\mathbb{Q}$ only by a constant factor. So it is enough to prove that there exists only finitely many fields $K/\mathbb{Q}$ of degree n containing $\sqrt{-1}$ with a given discriminant d. Such a field K has only complex embeddings; $\sigma : K \to \mathbb{C}$, total $n = 2r$ embeddings. Choose any one of them,τ. Consider the convex, centrally symmetric open subset of $\mathbb{C}^n$ given by

$$U = \left\{ (z_\sigma) \in \mathbb{C}^n \,\middle|\, |\Im(z_\tau)| < C\sqrt{d}, \Re(z_\tau) < 1, |z_\sigma| < 1 \text{ for } \sigma \neq \tau, \overline{\tau} \right\}$$

where C is an arbitrarily big constant which depends only on n. For a convenient choice of C, the volume of U will satisfy

$$vol(U) > 2^n\sqrt{d} = 2^n vol(\mathcal{O}_K)$$

where $vol(\mathcal{O}_K)$ is the volume of a fundamental mesh of the lattice obtained by embedding $\mathcal{O}_K$ in $\mathbb{C}^n$. By Minkowski's lattice point theorem, we can then find an $\alpha \in \mathcal{O}_K, \alpha \neq 0$, such that

$$|\Im(\tau\alpha)| < C\sqrt{d}, \;\; |\Re(\tau\alpha)| < 1, \;\; |\sigma\alpha| < 1 \;\; \forall \sigma \neq \tau, \overline{\tau} \qquad (\star)$$

Note that $N_{K/\mathbb{Q}}(\alpha) = \prod_\sigma |\sigma(\alpha)| \geq 1$ implies $|\tau(\alpha)| > 1$; thus $\Im(\tau(\alpha)) \neq 0$ so that the conjugates $\tau(\alpha)$ and $\overline{\tau}(\alpha)$ of α have to be distinct. Since $|\sigma(\alpha)| < 1$ for $\sigma \neq \tau, \overline{\tau}$, we have $\tau(\alpha) \neq \sigma(\alpha)$ for all $\sigma \neq \tau$. This implies $K = \mathbb{Q}(\alpha)$, because if $\mathbb{Q}(\alpha) \subsetneq K$ then the restriction $\tau|_{\mathbb{Q}(\alpha)}$ would admit an extension σ different from τ, contradicting $\tau(\alpha) \neq \sigma(\alpha)$.

Since the conjugates $\sigma(\alpha)$ of α are subject to condition $(\star)$, which only depends on d and n, the coefficients of the minimal polynomial of α are bounded once d and n are fixed. Thus every field $K/\mathbb{Q}$ of degree n and discriminant d is generated by one of the finitely many lattice points α in the bounded region U. Therefore there are only finitely many fields with given degree and discriminant. Hence there are only finitely many number fields of degree less than r and discriminant less than d for given integers $d, r \in \mathbb{N}$.