**Homework 9:** DEDEKIND DOMAINS

Questions marked with an * are optional, i.e. not for credit.

1) Suppose that $d \in \mathbf{Z}_{\neq 0,1}$ and that either $d \equiv 1 \bmod 4$ is square free, or $4|d$ and $d/4$ is square free. Let $\eta_d = (d + \sqrt{d})/2$. Show that $\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \mathbf{Z}[\eta_d]$, that $\mathcal{D}^{-1}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}} = (\sqrt{d})^{-1}\mathbf{Z}[\eta_d]$ and that $D_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}} = (d)$.

2) If $n$ is a positive integer and $\zeta_n$ denotes a primitive $n^{th}$ root of unity, show that $\mathcal{O}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}} = \mathbf{Z}[\zeta_n]$.

3) Let $K = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$.

(a) For each rational prime $p$ describe all the extensions of $\mathrm{ord}_p$ to $K$. Find the decomposition and inertia group in $\mathrm{Gal}(K/\mathbf{Q})$. [Hint: consider the different possibilities for $p$ modulo 20 and make use of Gauss' law of quadratic reciprocity.]

(b) What is the ring of integers $\mathcal{O}_K$ and the discriminant of $K/\mathbf{Q}$?

(c) Embed $\mathbf{Q}(\sqrt{-5})$ into $K$ by sending $\sqrt{-5}$ to $\sqrt{-1}\sqrt{5}$. Show that $K/\mathbf{Q}(\sqrt{-5})$ is unramified everywhere. Also show that in $\mathcal{O}_K$ we have

$$(2, 1 + \sqrt{-5}) = (1 + \sqrt{-1}).$$

Show also that the ideals $(3, 1+\sqrt{-5})$ and $(3, 1-\sqrt{-5})$ of $\mathbf{Z}[\sqrt{-5}]$ become principal in $\mathcal{O}_K$ and find generators.

4) Let $K = \mathbf{Q}(\sqrt{7}, \sqrt{13})$.

(a) Find $\mathcal{O}_K$ and $D_{K/\mathbf{Q}}$.

(b) Show that 3 splits completely in $K$.

(c) Show that $\mathcal{O}_K$ is not of the form $\mathbf{Z}[\alpha]$ for any $\alpha$. [Hint: if it were of this form then show that $\mathbf{F}_3^4 = \mathbf{F}_3[\overline{\alpha}]$ for some $\overline{\alpha} \in \mathbf{F}_3^4$.]

5) Let $K$ be a field and $\mathcal{P}$ a *finite* set of non-trivial valuations on $K$. Show that every ideal in $\mathcal{O}_{K,\mathcal{P}}$ is principal.

6*) Let $K$ be a field of characteristic different from 2. By a *quadratic space* over $K$ we mean a two dimensional vector space $V/K$ together with a non-degenerate symmetric bilinear form

$$q : V \times V \longrightarrow K.$$

We call $(V, q)$ and $(W, q')$ *equivalent* if there is a $K$-linear isomorphism $f : V \xrightarrow{\sim} W$ and an element $\alpha \in K$ which takes $q$ to $\alpha q'$, i.e.

$$q(x, y) = \alpha q'(f(x), f(y))$$

for all $x, y \in V$. If $V = K^2$ then we can write

$$q(x, y) = x^t Q y$$

for a symmetric matrix $Q \in M_{2\times 2}(K)$. Thus two symmetric matrices $Q$ and $Q'$ define equivalent quadratic spaces if

$$Q = \alpha F^t Q' F$$

for some$F \in GL_2(K)$ and $\alpha \in K$. Note that

$$(X_1, X_2) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = aX_1^2 + bX_1X_2 + cX_2^2$$

so that a quadratic space can also be represented as a quadratic form

$$aX_1^2 + bX_1X_2 + cX_2^2.$$

Two quadratic forms define equivalent quadratic spaces if one can be transformed into a scalar multiple of the other by a linear change of variables.

(a) We define the *discriminant* of a symmetric two by two matrix $Q$ over $K$ to be $-4 \det Q$. (This corresponds to defining the discriminant of $aX_1^2 + bX_1X_2 + cX_2^2$ to be $b^2 - 4ac$.) Show that the image of the discriminant in $K^\times/(K^\times)^2$ depends only on the equivalence class of the underlying quadratic space.

(b) Show that any quadratic space with discriminant $\delta$ is equivalent to one defined by the form $X_1^2 - \delta X_2^2$. Deduce that two quadratic spaces over $K$ are equivalent if and only if they have the same discriminant in $K^\times/(K^\times)^2$.

(c) If $L/K$ is a quadratic extension and if $\alpha \in K^\times$ show that we obtain a quadratic space by taking $L$ as the $K$-vector space and defining

$$q(x, y) = \mathrm{tr}_{L/K}(x(\sigma y))/2$$

where $\sigma$ is the non-trivial element of $\mathrm{Gal}(L/K)$. If $L = K(\sqrt{\delta})$, show that this quadratic space has discriminant $\delta$. Also show that every quadratic space over $K$ either arises in this way for some $L$, or it has discriminant 1. Deduce that there is a bijection between equivalence classes of quadratic spaces over $K$ with discriminant not equal to 1 and quadratic extensions $L/K$.[One can consider that the quadratic space with discriminant 1 corresponds to $K \oplus K$, a sort of degenerate quadratic extension. So it is perhaps better to work with etale quadratic $K$-algebras rather than with quadratic extensions.]

(d) If $\gamma \in L^\times$ and $x, y \in L$ show that

$$q(\sigma x, \sigma y) = q(x, y)$$

and that

$$q(\gamma x, \gamma y) = (\mathrm{N}_{L/K}\gamma) q(x, y).$$

Conversely if $a$ is a automorphism of the $K$-vector space $L$ and if $\beta \in K^\times$ such that

$$q(ax, ay) = \beta q(x, y)$$

for all $x, y \in L$, show that there is $\gamma \in L^\times$ such that $\mathrm{N}_{L/K}\gamma = \beta$ and either $ax = \gamma x$ for all $x \in L$, or $ax = \gamma(\sigma x)$ for all $x \in L$. [Hint: reduce to the case that $a1 = 1$.]

7*) By a *quadratic module* over $\mathbf{Z}$ we shall mean a free rank two $\mathbf{Z}$-module $M$ together with a non-degenerate symmetric bilinear form

$$q : M \times M \longrightarrow (1/2)\mathbf{Z}$$

such that $q(x, x) \in \mathbf{Z}$ for all $x \in M$. We call two quadratic modules $(M, q)$ and $(M', q')$ *equivalent* if there is an isomorphism $f : M \xrightarrow{\sim} M'$ which takes $q$ to $\pm q'$, i.e.

$$q(x, y) = \pm q'(f(x), f(y)).$$

for all $x, y \in M$ with $\pm$ independent of $x, y$. If $V = \mathbf{Z}^2$ then we can write

$$q(x, y) = x^t Q y$$

for a symmetric matrix $Q \in M_{2\times 2}((1/2)\mathbf{Z})$ whose diagonal entries are integers. Thus two such symmetric matrices $Q$ and $Q'$ define equivalent quadratic modules if

$$Q = \pm F^t Q' F$$

for some $F \in GL_2(\mathbf{Z})$. Note that

$$(X_1, X_2) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = aX_1^2 + bX_1X_2 + cX_2^2$$

so that a quadratic space can also be represented as a quadratic form

$$aX_1^2 + bX_1X_2 + cX_2^2$$

in $\mathbf{Z}[X_1, X_2]$. Two quadratic forms define equivalent quadratic modules if each can be transformed into $\pm 1$ times the other by a linear change of variables with $\mathbf{Z}$ coefficients. We call a quadratic module *primitive* if it can be represented by a quadratic form $aX_1^2 + bX_1X_2 + cX_2^2$ in which $a, b, c$ have no common factor.

(a) Show that $(M, q)$ is not primitive if and only if $(M, n^{-1}q)$ is also a quadratic module for some $n \in \mathbf{Z}_{>1}$.

(b) We define the *discriminant* of a symmetric two by two matrix $Q$ over $\mathbf{Z}$ to be $-4 \det Q$. (This corresponds to defining the discriminant of $aX_1^2 + bX_1X_2 + cX_2^2$ to be $b^2 - 4ac$.) Show that the discriminant depends only on the equivalence class of the underlying quadratic module. Also show that the discriminant is congruent to 0 or 1 modulo 4, and that any integer congruent to 0 or 1 modulo 4 is the discriminant of some primitive quadratic module. We call an integer $D$ a *fundamental* discriminant if either $D \equiv 1 \bmod 4$ and $D$ is square free, or $D \equiv 8$ or 12 modulo 16 and $D/4$ is square free.

If $M^\vee$ denotes the set of $x \in M \otimes_{\mathbf{Z}} \mathbf{Q}$ with

$$2q(x, M) \subset \mathbf{Z}$$

show that $M^\vee \supset M$ and that the absolute value of the discriminant equals the index $[M^\vee : M]$. Show moreover that the discriminant is positive if and only if there exists $0 \neq x \in M \otimes_{\mathbf{Z}} \mathbf{R}$ with $q(x, x) = 0$. (In this case we call $M$ *indefinite*, otherwise it is called *definite*.)

(c) If $(M, q)$ is any quadratic module with discriminant $D$ which is not a perfect square, show that we can find an embedding $M \hookrightarrow \mathbf{Q}(\sqrt{D})$ such that $q$ corresponds to

$$q(x, y) = (h/2)\mathrm{tr}_{\mathbf{Q}(\sqrt{D})/\mathbf{Q}}(x(\sigma y))$$

where $h \in \mathbf{Q}^\times$ and $\sigma$ is the non-trivial element of $\mathrm{Gal}(\mathbf{Q}(\sqrt{D})/\mathbf{Q})$.

(d) Let $d \neq 1$ be a fundamental discriminant and let $M \subset \mathbf{Q}(\sqrt{d})$ be a free rank two $\mathbf{Z}$-module. Set $\eta_d = (d + \sqrt{d})/2$. Show that $M$ has a basis $(a, b + c\eta_d)$ for some $a, b, c \in \mathbf{Q}_{\geq 0}$, and that $a$, $c$ and $(b \mod a)$ are uniquely determined by $M$. For any $f \in \mathbf{Q}$ define a bilinear form $q_{M,f}$ on $M$ by

$$q_{M,f}(x, y) = (f/(2ac))\mathrm{tr}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}(x(\sigma y)).$$

Show that $(M, q_{M,f})$ is a quadratic module if and only if $fa/c$, $f(2b + cd)/c$ and $f(b^2 + bcd + c^2d(d-1)/4)/ac$ are all integral and in this case it has discriminant $f^2d$. Deduce that if $(M, q_{M,f})$ is a quadratic module then $f \in \mathbf{Z}$. Also show that $fb/c$ is integral. [Hint: $f^2d \equiv f^2(2b + cd)^2/c^2 \bmod 4$.] Deduce that multiplication by elements of $\mathbf{Z}[f\eta_d]$ takes $M$ to itself. Further deduce that up to sign there is a unique $f$ which makes $(M, q_{M,f})$ primitive; that $(M, q_{M,f})$ is primitive if and only if

$$\{\alpha \in \mathbf{Q}(\sqrt{d}) : \ \alpha M \subset M\} = \mathbf{Z}[f\eta_d];$$

and that if $(M, q_{M,\pm 1})$ is a quadratic module then it is primitive. Conclude that any quadratic module with a fundamental discriminant is primitive.

If $\alpha \in \mathbf{Q}(\sqrt{d})^\times$ and if $\alpha M$ has a $\mathbf{Z}$-basis $(a', b' + c'\eta_d)$ with $a', b', c' \in \mathbf{Q}_{\geq 0}$ show that $a'c' = |\mathrm{N}_{\mathbf{Q}(\sqrt{d})/\mathbf{Q}}\alpha|_{\mathbf{R}} ac$. Deduce that $(M, q_{M,f})$ is equivalent to $(\alpha M, q_{\alpha M,f})$.

Conversely suppose that $M' \subset \mathbf{Q}(\sqrt{d})$ is a free $\mathbf{Z}$-module with basis $(a', b' + c'\eta_d)$ where $a', b', c' \in \mathbf{Q}_{\geq 0}$. Suppose also that $f' \in \mathbf{Z}$ and that $(M, q_{M,f})$ is equivalent to $(M', q_{M',f'})$. Show that there is an $\alpha \in \mathbf{Q}(\sqrt{d})^\times$ such that $\alpha M = M'$ or $\alpha M = \sigma M'$ and that $f' = \pm f$. [Hint: use 6) (d).]

Conclude that there is a bijection between equivalence classes of primitive quadratic modules with discriminant not a perfect square and equivalence classes of pairs $(L, M)$, where $L/\mathbf{Q}$ is a quadratic extension and $M \subset L$ is a free $\mathbf{Z}$-submodule of rank 2. Here we call two pairs $(L, M)$ and $(L', M')$ equivalent if there is an isomorphism of fields between $L$ and $L'$ under which $M$ corresponds to either $\alpha M'$

or $\alpha\sigma' M'$ for some $\alpha \in (L')^\times$. (We are writing $\sigma'$ for the non-trivial element of $\mathrm{Gal}(L'/\mathbf{Q})$.)

In particular conclude that there is a bijection between equivalence classes of primitive quadratic modules $(M, q)$ with $(M \otimes_{\mathbf{Z}} \mathbf{R}, q)$ positive definite and equivalence classes of pairs $(L, M)$ where $L/\mathbf{Q}$ is q quadratic extension with no embedding into $\mathbf{R}$ and $M \subset L$ is a free $\mathbf{Z}$-module of rank 2. Here we call two pairs $(L, M)$ and $(L', M')$ equivalent if there is an isomorphism of fields between $L$ and $L'$ under which $M$ corresponds to either $\alpha M'$ or $\alpha\sigma' M'$ for some $\alpha \in (L')^\times$.

(e) Show that the above construction sets up a bijection between equivalence classes of quadratic modules with fundamental discriminant $d \neq 1$ and the elements of the $\mathrm{Gal}(\mathbf{Q}(\sqrt{d})/\mathbf{Q})$ coinvariants of the ideal class group of $\mathbf{Z}[\eta_d]$. [The ideal class group of a quadratic extension of $\mathbf{Q}$ was first studied by Gauss, who defined it in terms integral binary quadratic forms. Amazingly he realized that the class group was an abelian group, although to define the composition law in terms binary quadratic forms is rather complicated.]

[There are variants on this that you can work out for yourself. One could define a narrower version of equivalence by requiring $q(x, y) = q'(f(x), f(y))$. Alternatively one could consider polarized quadratic modules, that it triples $(M, q, P)$ where $(M, q)$ is a quadratic module and where $P$ is a connected component of $((\wedge^2 M) \otimes_{\mathbf{Z}} \mathbf{R}) - \{0\}$. One can defined two polarised quadratic modules $(M, q, P)$ and $(M', q', P')$ to be equivalent if there is $f : M \xrightarrow{\sim} M'$ and $\mu = \pm 1$ such that

$$q'(f(x), f(y)) = \mu q(x, y)$$

and

$$(\wedge^2 f)P = \mu P'.$$

Then equivalence classes of polarized quadratic modules with fundamental discriminant $d$ correspond to elements of the class group of $\mathbf{Z}[\eta_d]$. One could also consider polarized quadratic modules with a a narrower definition of equivalence that required $\mu = 1$. These different notions correspond to working with the groups $GO(2)$, $O(2)$, $GO(2)^0$ and $SO(2) = O(2)^0$.]