Math 531 Tom Tucker
NOTES FROM CLASS 11/01

Let's prove a few things about discriminants, before moving on.

Lemma 26.1. *Let A be a Dedekind domain with field of fractions K, let $K \subseteq L$, and $K \subseteq E$ be separable, finite extensions that are linearly disjoint over K. Let R_E be the integral closure of A in E and let B be an integral extension of A with field of fractions L. Let $C = R_E B$ be the compositum of R_E and B in EL. Then $\Delta(C/R_E)R_E = \Delta(B/A)R_E$.*

Proof. It will suffice to show that for $\mathcal{P}$ be a prime of A and$S = A \setminus \mathcal{P}$, we have $S^{-1}R_E\Delta(S^{-1}C/S^{-1}R_E) = S^{-1}R_E\Delta(S^{-1}B/A_{\mathcal{P}})$, since

$$S^{-1}R_E\Delta(B/A) = S^{-1}R_E A_{\mathcal{P}}\Delta(B/A) = S^{-1}R_E(S^{-1}/A_{\mathcal{P}}).$$

Thus, we may assume that $A = A_{\mathcal{P}}$, that $B = S^{-1}B$, $R_E = S^{-1}R_E$, $C = S^{-1}C$. Let $w_1, \ldots, w_n$ be basis for B over A (we have assumed now that A is a DVR). Then $w_1, \ldots, w_n$ must also generate C as an R_E-module. Moreover, since $[EL : E] = [L : K] = n$, since E and L are linearly disjoint. Hence, $w_1, \ldots, w_n$ is a basis for C over R_E. We can use it to calculate both discriminants then. It is clear that $\mathrm{T}_{L/K}(y) = \mathrm{T}_{LE/L}(y)$ for any $y \in L$, since the trace is determined by how yw_i can be written in terms of the w_i. We see then that

$$\Delta(C/B) = \det[\mathrm{T}_{LE/L}(w_i w_j)] = \det[\mathrm{T}_{L/K}(w_i w_j)] = \Delta(R_E/A),$$

and we are done. □

Proposition 26.2. *Let A be a Dedekind domain with field of fractions K, let $K \subseteq L$, and $K \subseteq E$ be separable, finite extensions that are linearly disjoint over K. Let R_E be the integral closure of A in E and let R_L be the integral closure of A in L. Suppose that $A\Delta(R_E/A) + A\Delta(R_L/A) = 1$. Then $C = R_E R_L$ is Dedekind.*

Proof. Let $\mathcal{M}$ be a prime in $R_E R_L$ such that $\mathcal{M} \cap A = \mathcal{P}$. Since $A\Delta(R_E/A) + A\Delta(R_L/A) = 1$, either $A\Delta(R_E/A)$ or $A\Delta(R_L/A)$ is contained in $\mathcal{P}$. We may suppose WLOG that $A\Delta(R_L/A)$ isn't contained in $\mathcal{P}$. It follows from the Lemma above that for any $\mathcal{Q} \cap R_E$ that is prime and lies over $\mathcal{P}$, the ideal $R_E\Delta(C/R_E)$ doesn't contain $\mathcal{Q}$. Thus, if $S = R_E \setminus \mathcal{Q}$, then $S^{-1}C$ is Dedekind, so $\mathcal{M}$ is invertible. So every prime $\mathcal{M}$ of C is invertible and C must be Dedekind. □

We were in the middle of proving the following...

Proposition 26.3. *Let A be a Dedekind domain with field of fractions K, let $K \subseteq L$, and $K \subseteq E$ be separable, finite extensions that are linearly disjoint over K. Let R_E be the integral closure of A in E and*

let R_L be the integral closure of A in L. Suppose that $A\Delta(R_E/A) + A\Delta(R_L/A) = 1$. Then $C = R_E R_L$ is Dedekind.

Proof. Let $\mathcal{M}$ be a prime in $R_E R_L$ such that $\mathcal{M} \cap A = \mathcal{P}$. Since $A\Delta(R_E/A) + A\Delta(R_L/A) = 1$, either $A\Delta(R_E/A)$ or $A\Delta(R_L/A)$ is not contained in $\mathcal{P}$. We may suppose WLOG that $A\Delta(R_L/A)$ doesn't isn't contained in $\mathcal{P}$. It follows from the Lemma above that for any $\mathcal{Q} \cap R_E$ that is prime and lies over $\mathcal{P}$, the ideal $R_E\Delta(C/R_E)$ doesn't contain $\mathcal{Q}$. Thus, if $S = R_E \setminus \mathcal{Q}$, then $S^{-1}C$ is Dedekind, so $\mathcal{M}$ is invertible. So every prime $\mathcal{M}$ of C is invertible and C must be Dedekind. □

Lemma 26.4. *Let $K \subset K' \subset L$ be finite separable field extensions. Let A be Dedekind with field of fractions K, and let R_L and $R_{K'}$ be integral closures of A in L and K' respectively. Let $\mathcal{Q} \subseteq R_{K'}$ be a maximal ideal with $\mathcal{Q} \cap A = \mathcal{P}$. Then $\Delta(R_L/A) + \mathcal{P} = 1$ implies $\Delta(R_L/R_{K'}) + \mathcal{Q} = 1$*

Proof. It suffices to show that $\mathcal{Q}$ doesn't ramify in R_L whenever $\mathcal{P}$ doesn't ramify in R_L. So suppose $\mathcal{P}$ doesn't ramify in R_L; then $\mathcal{P}R_L$ is a product of distinct primes in R_L. We also know that for some ideal I in $R_{K'}$ we have

$$\mathcal{P}R_L = \mathcal{P}R_{K'}R_L = I\mathcal{Q}R_L,$$

so $\mathcal{Q}$ factors into distinct primes also, which means that $\Delta(R_L/R_{K'}) + \mathcal{Q} = 1$. □

Theorem 26.5. *Let A be a Dedekind domain with field of fractions K, let $K \subseteq L$, and $K \subseteq E$ be separable, finite extensions. Let R_E be the integral closure of A in E and let R_L be the integral closure of A in L. Suppose that $A\Delta(R_E/A) + A\Delta(R_L/A) = 1$. Then $C = R_E R_L$ is Dedekind.*

Proof. Let $K' = E \cap L$ and let $R_{K'}$ be the integral closure of A in K' By Lemma 26.4, we must have $R_{K'}\Delta(R_E/R_{K'}) + R_{K'}\Delta(R_L/R_{K'}) + \mathcal{Q} = 1$ for any prime $\mathcal{Q}$ of $R_{K'}$, so we must have $R_{K'}\Delta(R_E/R_{K'}) + R_{K'}\Delta(R_L/R_{K'}) = 1$. Proposition 26.3 then applies to $R_E R_L$, when R_E and R_L are considered as extensions of $R_{K'}$. □

********** Now, let's move on to the class group. Recall that for any integral domain R, we have notion of invertible ideals (recall that it is a fractional ideal with an inverse) and that we have an exact sequence

$$0 \longrightarrow \mathrm{Pri}(R) \longrightarrow \mathrm{Inv}(R) \longrightarrow \mathrm{Pic}(R) \longrightarrow 0.$$

where $\mathrm{Pri}(R)$ is the set of principal ideals of R, $\mathrm{Inv}(R)$ is set of invertible ideals of R, and the group law is multiplication of fractional ideals. When R is Dedekind, we call $\mathrm{Pic}(R)$ the class group of R and denote it

as $\mathrm{Cl}(R)$. When R is the integral closure $\mathcal{O}_L$ of $\mathbb{Z}$ in some number field L, we often write $\mathrm{Cl}(L)$ for $\mathrm{Cl}(\mathcal{O}_L)$. We also write $\Delta(L)$ for $\Delta(\mathcal{O}_L/\mathbb{Z})$. We want to prove the following.

Theorem 26.6. *Let L be a number field. Then $\mathrm{Cl}(L)$ is finite.*

We've already shown this $\mathbb{Z}[i]$. We showed that $\mathrm{Cl}(\mathbb{Z}[i]) = 1$, i.e. that it is a principal ideal domain. On the other hand, we've seen that $\mathrm{Pic}(\mathbb{Z}[\sqrt{19}]) \neq 1$ (this ring isn't Dedekind, but later we'll see Dedekind rings with nontrivial class groups.

How did we show that $\mathrm{Cl}(\mathbb{Z}[i]) = 1$? We took advantage of the fact that $\mathbb{Z}[i]$ forms a sublattice of $\mathbb{C}$. We'll try to do that in general.

Here is the idea... If we have a number field L of degree n over $\mathbb{Q}$, then we have n different embeddings of L into $\mathbb{C}$. They can be obtained by fixing one embedding $L \longrightarrow \mathbb{C}$ and then conjugating this embedding by elements in the cosets of H_L in $\mathrm{Gal}(M/\mathbb{Q})$ for M some Galois extension of $\mathbb{Q}$ containing L. We'll use these to make B a full lattice in $\mathbb{R}^n$. What is a full lattice?

Definition 26.7. A lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module whose rank as a $\mathbb{Z}$-module is the equal to the dimension of the $\mathbb{R}$-vector space generated by $\mathcal{L}$. A full lattice $\mathcal{L} \subset \mathbb{R}^n$ is a free $\mathbb{Z}$-module of rank n that generates $\mathbb{R}^n$ as a $\mathbb{R}$-vector space.

Example 26.8.
(1) $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ is *not* a full lattice of $\mathbb{R}^2$ under the embedding $1 \mapsto 1$ and $\theta \mapsto \sqrt{3}$, since it generates an $\mathbb{R}$-vector space of dimension 1.
(2) $\mathbb{Z}[i]$ is full lattice in $\mathbb{R}^2$ where $\mathbb{R}^2$ is $\mathbb{C}$ considered as an $\mathbb{R}$-vector space with basis $1, i$ over $\mathbb{R}$.

On the other hand, we can send $\mathbb{Z}[\theta]$ where $\theta^2 = 3$ into $\mathbb{R}^2$ in such a way that it is a full lattice in the following way. Let $\phi : 1 \mapsto (1, 1)$ and $\phi : \theta :\longrightarrow (\sqrt{3}, -\sqrt{3})$. In this case, we must generated $\mathbb{R}^2$ as an $\mathbb{R}^2$ vector space since $(1, 1)$ and $(\sqrt{3}, -\sqrt{3})$ are linearly independent.

There are two different types of embeddings of L into $\mathbb{C}$. There are the real ones and the complex ones. An embedding $\sigma : L \longrightarrow \mathbb{C}$ is real if $\overline{\sigma(y)} = \sigma(y)$ for every $y \in L$ (the bar here denotes complex conjugation) and is complex otherwise. How can we tell which is which?

Suppose we have a number field L. We can write $L \cong \mathbb{Q}[X]/f(X)$ for some monic irreducible polynomial L with integer coefficients. Then by the Chinese remainder theorem $\mathbb{R}[X]/f(X) \cong \bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X)$ where the f_i have coefficients in $\mathbb{R}$, are irreducible over $\mathbb{R}$, and $f_1 \dots f_m = g$ (note that the f_i are distinct since L is separable over $\mathbb{Q}$). We also know that each f_i is of degree 1 or 2. When f_i has degree 1, then $\mathbb{R}[X]/f_i(X)$

is isomorphic to $\mathbb{R}$ and when f_i has degree 2, then $\mathbb{R}[X]/f_i(X)$ is isomorphic to $\mathbb{C}$. Since $\mathbb{Q}$ has a natural embedding into $\mathbb{R}$, we obtain a natural embedding of

$$j : L \cong \mathbb{Q}[X]/f(X) \longrightarrow \bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X).$$

Composing j with projection onto the i-th factor of

$$\bigoplus_{i=1}^{m} \mathbb{R}[X]/f_i(X)$$

then gives a map from $L \longrightarrow \mathbb{R}$ or $L \longrightarrow \mathbb{C}$. In fact, when $\deg f_i = 2$ and $\mathbb{R}[X]/f_i(X)$ is $\mathbb{C}$ we get two embeddings by composing with conjugation. The image of L is the same for these two embeddings, so we will want to link these two in some way...

Let's order the embeddings $\sigma_1, \ldots, \sigma_n$ ($n = [L : \mathbb{Q}]$) in the following way. We let $\sigma_1, \ldots, \sigma_s$ be real embeddings. The remaining embeddings come in pairs as explained above, so for $i = r+1, r+3, \ldots$, we let σ_i be a complex embedding and let $\sigma_{i+1} = \overline{\sigma_{i+1}}$. We let s be the number of complex embeddings. We have $r + 2s = n$.

Now, we can embed $\mathcal{O}_L$ into $\mathbb{R}^n$ by letting

$$\begin{aligned} h(y) &= (\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \Re(\sigma_{r+1}(y)), \Im(\sigma_{r+1}(y)), \ldots, \Re(\sigma_{r+2(s-1)}(y)), \Im(\sigma_{r+2(s-1)}(y))) \\ &\quad = \big(\sigma_1(y), \ldots, \sigma_r(y), \\ &\quad \frac{\sigma_{r+1}(y) + \sigma_{r+2}(y)}{2}, \frac{\sigma_{r+1}(y) - \sigma_{r+2}(y)}{2i}, \ldots, \\ &\quad \frac{\sigma_{r+2(s-1)}(y) + \sigma_{r+2(s-1)}(y)}{2}, \frac{\sigma_{r+2(s-1)}(y) - \sigma_{r+2(s-1)+1}(y)}{2i}\big). \end{aligned} \tag{1}$$

Let us also denote as h_i the map $h : \mathcal{O}_L \longrightarrow \mathbb{R}$ given by composing h with projection p_i onto the i-th coordinate of $\mathbb{R}^n$.

We will continue to use h and h_i as defined above. We will also continue to let s and r be as above and to let $n = r + 2s$ be the degree $[L : \mathbb{Q}]$.