Math 568 Tom Tucker
NOTES FROM CLASS 11/10

Note: I organized this a little bit differently from in class.

Recall that if L and E are finite extensions of K, we say that L ane E are linearly disjoint over K If

$$[EL : K] = [E : K][L : K].$$

Note that this is stronger than saying $E \cap L = K$. For example, if $E = \mathbb{Q}(\sqrt[3]{5})$ and $L = \mathbb{Q}(\xi_3 \sqrt[3]{5})$, then $E \cdot L$ has degree six over $\mathbb{Q}$, not degree nine, so E and L are not linearly disjoint over $\mathbb{Q}$.

Note however that if L or E is Galois over K, then E and L *are* linearly disjoint over K if and only if $E \cap L = K$. The key fact here is that if E is Galois then $E = K(\theta)$ for some θ such that K contains all the conjugates of θ and thus contains the coefficients of any factor of the minimal polynomial for θ.

Let's now introduce semidirect products.

Let G be group. We say that G is the semidirect product $N \rtimes H$ if

- H is a subgroup of G and N is a normal subgroup of G;
- $HN = G$; and
- $H \cap N = \{e\}$.

We have the following simple fact about composita of extensions.

Proposition 17.1. *Let L and E be finite, separable, linearly disjoint field extensions of a field K. Suppose that L is Galois over K. Then*

$$\mathrm{Gal}(EL/K) \cong \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(EL/L).$$

Proof. Since L is Galois over K and E, L are disjoint over K, we have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(EL/E)$. Now, let $N = \mathrm{Gal}(EL/E)$ and let $H = \mathrm{Gal}(EL/L)$. Then N is normal. Since K is the fixed field of HN, we see that $HN = \mathrm{Gal}(EL/K)$. It follows that $H \cap N = \{e\}$ by looking at degrees of extensions. □

Proposition 17.2. *Let ξ_m be a primitive m-th root of unity. Then $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$ (the multiplicative units of $\mathbb{Z}/m\mathbb{Z}$).*

Proof. Let ξ_m be a primitive m-th root of unity. Then for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}$, we have $\sigma(\xi_m) = \xi_m^i$ where $i \in (\mathbb{Z}/m\mathbb{Z})^*$. The map $\theta : \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ sending σ to i is an isomorphism since all ξ_m^i, where $i \in (\mathbb{Z}/m\mathbb{Z})^*$, are conjugate to ξ_m. □

Proposition 17.3. *Let L be a field containing a primitive m-th root of unity ξ_m, let $x^m - a$ be irreducible over L, and let M be a spitting field of $x^m - a$ over L. Then $\mathrm{Gal}(L/M)$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Let α be a root of $x^m - a$. Then $\theta : \sigma \mapsto \sigma(\alpha)/\alpha$ is an isomorphism from $\mathrm{Gal}(M/L)$ to the m-th roots of unity in L. Since the group of m-th roots of unity in L is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, we are done. □

Theorem 17.4. *Suppose that $x^m - a$ is irreducible over $\mathbb{Q}$ and that $\mathbb{Q}(\sqrt[m]{a})$ and $\mathbb{Q}(\xi_m)$ are linearly disjoint over $\mathbb{Q}$. Let M be the splitting field of $x^m - a$ over $\mathbb{Q}$. Then $\mathrm{Gal}(M/\mathbb{Q})$ is isomorphic to the semidirect product $\mathbb{Z}/m\mathbb{Z} \rtimes (\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. This follows from Propositions 17.1, 17.2, and 17.3.

□

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

Lemma 17.5. *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 17.6. *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 17.7. *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. □

********************** 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, all fractional ideals are invertible and we write this as

$$0 \longrightarrow \mathrm{Pri}(R) \longrightarrow \mathrm{Fr}(R) \longrightarrow \mathrm{Cl}(R) \longrightarrow 0.$$

We call the quotient $\mathrm{Cl}(R)$ above the class group of 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 17.8. *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 17.9. 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 17.10.
(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 $\mathbb{R}$.

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.

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

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

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 $[L : \mathbb{Q}]$.