Math 676. Discriminants and étale algebras

Let A be a noetherian domain with fraction field F. Let B be an A-algebra that is finitely generated and torsion-free as an A-module with B also locally free as an A-module (that is, $B_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module for every maximal ideal $\mathfrak{m}$ of A). Since localization at a prime $\mathfrak{p}$ of A may be achieved by first localizing at a maximal $\mathfrak{m}$ containing $\mathfrak{p}$ and then localizing at the prime $\mathfrak{p}A_{\mathfrak{m}}$ of $A_{\mathfrak{m}}$, we see that the $A_{\mathfrak{p}}$-algebra $B_{\mathfrak{p}}$ is a finite free $A_{\mathfrak{p}}$-module for every prime ideal $\mathfrak{p}$ of A.

As we saw in the handout on existence of discriminant ideals, the $S^{-1}A$-algebra $S^{-1}B$ satisfies the same hypotheses for any multiplicative set S of A with $0 \notin S$, and that under these assumptions on B there is a unique ideal $\mathfrak{d}_{B/A}$ of A such that $\mathfrak{d}_{B/A}A_{\mathfrak{m}} = \mathrm{disc}(B_{\mathfrak{m}}/A_{\mathfrak{m}})$ for every maximal ideal $\mathfrak{m}$ of A (and even for every prime ideal $\mathfrak{p}$ of A). This is the *discriminant ideal* of B over A, and in that handout we worked out several properties of the discriminant ideal (such as behavior with respect to localization, extension of scalars to another noetherian domain, and tensor product of two such A-algebras). In this handout we will be particularly interested in studying the case when the discriminant ideal is equal to A, as this provides a powerful technique for proving that certain abstractly constructed A-algebras enjoy good properties.

Here is a question: if a number field L is a compositum of two subfields K and K', when does it happen that $\mathscr{O}_L = \mathscr{O}_K\mathscr{O}_{K'}$? That is, when is $\mathscr{O}_L$ spanned over $\mathbf{Z}$ by products xx' with $x \in \mathscr{O}_K$ and $x' \in \mathscr{O}_{K'}$? With our later work in ramification theory it will become obvious that if K and K' are non-isomorphic quadratic fields over $\mathbf{Q}$ with a common ramified prime p then frequently $[\mathscr{O}_{KK'} : \mathscr{O}_K\mathscr{O}_{K'}]$ is divisible by p (and so this lattice index cannot equal 1). In general the relation between $\mathscr{O}_{KK'}$ and $\mathscr{O}_K\mathscr{O}_{K'}$ is subtle, but the theory of the discriminant will provide a powerful tool to understand the situation in some cases.

1. Étale algebras

We work with A and B as above. The A-algebra B (satisfying the preceding module hypotheses!) is said to be *finite étale* if $\mathfrak{d}_{B/A} = A$.

Lemma 1.1. *Let B be a finite étale A-algebra. If $A \to A'$ is a map to another noetherian domain, then the A'-algebra $B' = A' \otimes_A B$ is finite étale over A'. Also, if S is any multiplicative set of A with $0 \notin S$ then $S^{-1}B$ is a finite étale $S^{-1}A$-algebra.*

In the previous handout it was shown that B' is a finitely generated and torsion-free A'-module that is moreover locally free. Hence, $\mathfrak{d}_{B'/A'}$ makes sense.

Proof. These are immediate from the identities $\mathfrak{d}_{B/A}A' = \mathfrak{d}_{B'/A'}$ and $S^{-1}\mathfrak{d}_{B/A} = \mathfrak{d}_{S^{-1}B/S^{-1}A}$. ∎

Lemma 1.2. *Let A_1 and A_2 be two A-algebras that are finitely generated and torsion-free as A-modules, and assume that each is locally free as an A-module. The A-algebra $A_1 \times A_2$ is finite étale if and only if A_1 and A_2 are each finite étale over A, and the A-algebra $A_1 \otimes_A A_2$ is finite étale over A if and only if A_1 and A_2 are finite étale over A.*

In the previous handout it was shown that $A_1 \otimes_A A_2$ is finitely generated and torsion-free as an A-module, and that it is locally free as such.

Proof. By the previous handout, $\mathfrak{d}_{A_1\times A_2/A} = \mathfrak{d}_{A_1/A}\mathfrak{d}_{A_2/A}$ and $\mathfrak{d}_{A_1\otimes_A A_2/A} = \mathfrak{d}_{A_1/A}^{n_2}\mathfrak{d}_{A_2/A}^{n_1}$ where $n_i \geq 1$ is the A-rank of A_i (the common rank of the free $A_{\mathfrak{p}}$-module $(A_i)_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of A). Hence, the "if" directions are obvious, and for the converses we just have to prove that if I and J are two ideals in a domain A such that $IJ = A$ then $I = J = A$. This is obvious, since $IJ \subseteq I$ and $IJ \subseteq J$. ∎

Now we finally come to the point of these efforts. Let B be as above, and assume that A is integrally closed in its fraction field F. Localizing B at $A - \{0\}$ gives $F \otimes_A B$, so this is finite étale over the field F and it contains B as a subring. As was explained in lecture, a finite étale algebra over a *field* is the same thing as a finite product of finite separable field extensions! Hence, $F \otimes_A B = F_1 \times \cdots \times F_n$ with the F_i's finite *separable* field extensions of F (and, as we saw in lecture, such a product decomposition of the F-finite commutative ring $F \otimes_A B$ is unique up to ordering of the factors;the F_i's are the quotients of $F \otimes_A B$ by the principal ideals $(1 - \varepsilon)$ for the finitely many primitive idempotents ε in the ring $F \otimes_A B$).

Thus, the integral closure A_i of A in F_i is a finitely generated (and torsion-free) A-module. It is not *a priori* clear if the A_i's are locally free as A-modules (though this is obvious if A is Dedekind). Since B is an A-algebra that is finitely generated as an A-module, by the "determinant trick" every element of B satisfies a monic polynomial equation with coefficients in A. Hence, the image of B in each factor F_i of $F \otimes_A B$ is an A-subalgebra of F_i whose elements are integral over A. That is, the image of B in each F_i lies in A_i, and hence we get a containment

$$B \subseteq A_1 \times \cdots \times A_n$$

inside of $F \otimes_A B = \prod F_i$. Here is the wonderful fact:

Theorem 1.3. *If B is a finite étale A-algebra and A is Dedekind, then $B = \prod A_i$. In particular, if a domain B is a finite étale A-algebra and A is Dedekind then B is Dedekind.*

The first part of this theorem is true without a Dedekind restriction on A, and the second part is true with "integrally closed" replacing "Dedekind," but the proof in such generality requires stronger methods in commutative algebra.

Proof. We want to prove that the inclusion $B \subseteq \prod A_i$ of finitely generated and torsion-free A-modules is an equality, so it suffices to check this after localizing at maximal ideals of A. This localization process preserves the hypotheses on B, and is compatible with the formation of the A_i's, so we may now assume that A is local. Hence, B is free as an A-module. Since A is now a discrete valuation ring, the A_i's are also free as A-modules. The inclusion $B \subseteq \prod A_i$ becomes an equality upon extending scalars by $A \to F$, so if we choose an A-basis $\{e_r\}$ for B and $\{e'_r\}$ for $\prod A_i$ then the matrix M whose columns give the A-coordinates for each e_r in terms of the e'_s's is an invertible matrix if and only if $B = \prod A_i$. It is clear from matrix considerations with the trace forms on B and $\prod A_i$ relative to A that

$$\mathrm{disc}(B/A) = \mathrm{disc}((A_1 \times \cdots \times A_n)/A) \cdot \det(M)^2 A.$$

By hypothesis, $\mathrm{disc}(B/A) = A$. Hence, $\det(M)A = A$, so $\det(M) \in A^\times$. ∎

We immediately get a nice corollary:

Corollary 1.4. *Let K be a number field, and $\mathscr{O} \subseteq \mathscr{O}_K$ an order. If $d = \mathrm{disc}(\mathscr{O}/\mathbf{Z})$ then $\mathscr{O}[1/d] = \mathscr{O}_K[1/d]$. In particular, $\mathscr{O}[1/d]$ is Dedekind and the only prime factors of $[\mathscr{O}_K : \mathscr{O}]$ are primes that divide d.*

Thus, if we compute some specific order then as long as we wish to study primes away from the divisors of the discriminant of the order then the ring behaves "as if" it were the ring of integers.

Proof. The discriminant is compatible with localization, so $\mathrm{disc}(\mathscr{O}[1/d]/\mathbf{Z}[1/d]) = d\mathbf{Z}[1/d] = \mathbf{Z}[1/d]$, so the domain $\mathscr{O}[1/d]$ is a finite étale $\mathbf{Z}[1/d]$-algebra. ∎

To give a further corollary of much significance in practice, let A be Dedekind with field of fractions F, and let L and L' be finite separable extensions of F. The F-algebra $L \otimes_F L'$ is a product of finitely many finite separable extensions of F (either because it is a finite étale F-algebra, being a tensor product of two such, or "by hand": we write $L = F[T]/(h)$ for an irreducible separable $h \in F[T]$ and then have $L \otimes_F L' = L'[T]/(h)$ and $h \in L'[T]$ may be reducible but it is still separable). Thus, we have a finite product decomposition $L \otimes_F L' = \prod F_i$ with F_i/F a finite separable extension. An element in $\prod F_i$ is integral over A if and only if each of its components is integral over A (why?), and so the integral closure of A in $\prod F_i$ is $\prod A_i$ with A_i equal to the integral closure of A_i in F_i (so each A_i is a Dedekind domain finite over A).

Corollary 1.5. *Assume A is Dedekind. Let B be the integral closure of A in L and let B' be the integral closure of A in L', so B and B' are finitely generated torsion-free A-modules that are locally free as such. Also, $F \otimes_A B = L$ and $F \otimes_A B' = L'$, so $F \otimes_A (B \otimes_A B') \simeq L \otimes_F L'$; that is, the natural map $B \otimes_A B' \to L \otimes_F L'$ is injective. We use this to identify $B \otimes_A B'$ with an A-subalgebra of $L \otimes_F L'$.*

If the nonzero ideals $\mathfrak{d}_{B/A}$ and $\mathfrak{d}_{B'/A}$ of A are relatively prime then $B \otimes_A B' = \prod A_i$ inside of $L \otimes_F L' = \prod F_i$. In particular, if $L \otimes_F L'$ is a field and $\mathfrak{d}_{B/A}$ is coprime to $\mathfrak{d}_{B'/A}$ then $B \otimes_A B'$ is the integral closure of A in the field $L \otimes_F L'$.

Before we prove the corollary, we note that it is a very powerful result: as an example, if K and K' are number fields such that $K \otimes_{\mathbf{Q}} K'$ is a field (to be denoted KK') and such that $\mathrm{disc}(K/\mathbf{Q})$ and $\mathrm{disc}(K'/\mathbf{Q})$ are relatively prime (where, as usual, we abuse notation and write $\mathrm{disc}(K/\mathbf{Q})$ to denote $\mathrm{disc}(\mathscr{O}_K/\mathbf{Z})$, and likewise for k'), then $\mathscr{O}_{KK'} = \mathscr{O}_K \otimes_{\mathbf{Z}} \mathscr{O}_{K'}$. In particular, in such cases $\mathscr{O}_{KK'}$ is the subring of KK' generated by $\mathscr{O}_K$ and $\mathscr{O}_{K'}$, and moreover $\mathrm{disc}(KK'/\mathbf{Q}) = \mathrm{disc}(K/\mathbf{Q})^{[K':\mathbf{Q}]}\mathrm{disc}(K'/\mathbf{Q})^{[K:\mathbf{Q}]}$. In the next section we will take up such examples in more detail.

Proof. As in the setup preceding Theorem 1.3, we have the inclusion $B \otimes_A B' \subseteq \prod A_i$ inside of $L \otimes_F L' = \prod F_i$ because the image of $B \otimes_A B'$ in each F_i is an A-subalgebra that is finitely generated as an A-module (and hence is contained in A_i). Our task is therefore to prove that this inclusion is an equality. As usual, we may work locally on A since the formation of everything in sight is compatible with such localization. Hence, we can assume that A is local. In particular, one of the ideals $\mathfrak{d}_{B/A}$ or $\mathfrak{d}_{B'/A}$ is equal to A since they are coprime ideals in the local ring A. By renaming, we may suppose $\mathfrak{d}_{B/A} = A$. This says that B is a finite étale A-algebra. Hence, by Lemma 1.1, $B \otimes_A B'$ is a finite étale B'-algebra. Since B' is Dedekind, by Theorem 1.3 it follows that $B \otimes_A B'$ is the integral closure of B' in the finite étale L'-algebra $L \otimes_F L'$. Integrality over B' is equivalent to integrality over A since B' is integral (and even module-finite) over A, so $B \otimes_A B'$ is the integral closure of A in $L \otimes_F L'$. ∎

Let us conclude this section with an example. Let n_1 and n_2 be relatively prime positive integers, and let $n = n_1 n_2$. The splitting field $K = \mathbf{Q}(\zeta_n)$ for $X^n - 1$ over $\mathbf{Q}$ contains subfields $\mathbf{Q}(\zeta_{n_1})$ and $\mathbf{Q}(\zeta_{n_2})$ that are intrinsically described (without the artifice of the ζ's) as the splitting fields for $X^{n_1} - 1$ and $X^{n_2} - 1$ over $\mathbf{Q}$ inside of K. The inclusions of these subfields into K define a natural map of $\mathbf{Q}$-algebras

$$\mathbf{Q}(\zeta_{n_1}) \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_{n_2}) \to \mathbf{Q}(\zeta_n)$$

and this is surjective because a primitive nth root of unity may be obtained as a suitable product of powers of any primitive n_1th root of unity and primitive n_2th root of unity (here we use that $\gcd(n_1, n_2) = 1$). However, the two sides of this surjection have respective $\mathbf{Q}$-vector space dimensions $\phi(n_1)\phi(n_2)$ and $\phi(n)$, so by the multiplicativity of Euler's function we conclude that this is an isomorphism! Hence:

Corollary 1.6. *The ring of integers of $\mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$, and the prime factors of its discriminant are precisely the prime factors of n.*

Proof. The case when n is a prime power is known, and so we induct on the prime factorization of n. In view of Corollary 1.5 and the preceding calculations with cyclotomic fields, it remains to observe that the natural map

$$\mathbf{Z}[\zeta_{n_1}] \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_{n_2}] \to \mathbf{Z}[\zeta_n]$$

is an isomorphism for $n = n_1 n_2$ with relatively prime positive integers n_1 and n_2 (and we may then use the formula for the discriminant of a tensor-product algebra to read off the discriminant of $\mathbf{Z}[\zeta_n]$, and more specifically its prime factors). To prove that this map is an isomorphism, the surjectivity goes as in the field case and for the injectivity we may use torsion-freeness to reduce to injectivity after extensing scalars to $\mathbf{Q}$. This latter situation recovers exactly the analogous map on the level of cyclotomic fields that we have shown to be injective for dimension reasons. ∎

2. Linear disjointness

In view of the preceding section, it is an interesting condition on a pair of finite extensions L and L' over a field F to require that $L \otimes_F L'$ is again a field.

Definition 2.1. A pair of finite extensions L and L' over a field F are *linearly disjoint* over F if $L \otimes_F L'$ is a field.

As an example, if A is a Dedekind domain with fraction field F and L and L' are a pair of linearly disjoint finite separable extensions of F with B and B' denoting the integral closure of A in L and L' respectively, then the integral closure of A in the field $L \otimes_F L'$ is $B \otimes_A B'$ if $\mathfrak{d}_{B/A} + \mathfrak{d}_{B'/A} = A$.

The concept of linear disjointness can be defined for general pairs of field extensions (one requires that $L \otimes_F L'$ is a domain), but the uses of this generality are a bit more technical and the discussion that follows does not carry over. The reason that linear disjointness is especially interesting for us is due to:

Lemma 2.2. *Suppose that L and L' are linearly disjoint over a field F. If $i : L \to M$ and $i' : L' \to M$ are F-embeddings into an extension M of F, then the F-isomorphism class of the compositum $i(L)i'(L') \subseteq M$ is independent of i and i'.*

Proof. Consider the map of F-algebras $L \otimes_F L' \to M$ given by $x \otimes x' \mapsto i(x)i'(x')$. The image is $i(L)i'(L')$, and since $L \otimes_F L'$ is a field the kernel must be 0. Hence, $i(L)i'(L')$ is F-isomorphic to the abstract field $L \otimes_F L'$ that has nothing to do with i or i'. ■

The conclusion of Lemma 2.2 is often false without a linear disjointness condition. For example, if $L = L'$ is a non-Galois separable finite extension of F and M is a Galois closure, then L and L' are certainly *not* linearly disjoint over F (as $L \otimes_F L'$ admits a nonzero quotient L with nonzero kernel) and we can take $i = i'$ or we can take i' so that $i'(L')$ is not contained in $i(L)$. The two resulting composites do not even have the same degree over F, so they are certainly not F-isomorphic. If $[L : F]$ is prime then in the second case the two subfields $i(L)$ and $i'(L')$ inside of M have "trivial" intersection F for degree reasons, so we see that such a property is usually much weaker than linear disjointness.

Intuitively, linear disjointness ensures that the formation of the compositum of the two fields over F is an intrinsic operation that does not depend (up to non-unique isomorphism!) on how the two fields are put into a common extension field over F.

Here is a convenient criterion for linear disjointness.

Theorem 2.3. *Let M/F be an extension of fields and let L and L' be subextensions with finite degree over F. If L and L' are linearly disjoint over F then $L \cap L' = F$. If one of L or L' is Galois over F then the condition $L \cap L' = F$ is also sufficient for L and L' to be linearly disjoint over F.*

Proof. First assume linear disjointness holds, so the map $L \otimes_F L' \to M$ is an isomorphism onto LL'. Pick $x \in L \cap L'$, so $1 \otimes x$ and $x \otimes 1$ have the same image in M and hence coincide in $L \otimes_F L'$. We may identify $L \otimes_F L'$ with an F-subspace of $M \otimes_F M$, so to prove $x \in F$ we are reduced to the problem of proving that if F is a field and A is an F-algebra then $a \otimes 1 = 1 \otimes a$ in $A \otimes_F A$ for $a \in A$ if and only if $a \in F$. The "if" direction is trivial (and is not the implication we need), and for the converse we consider the expansion $a = \sum c_i e_i$ with respect to an F-basis $\{e_i\}$ of A such that some e_{i_0} is equal to 1. Thus, the vectors $1 \otimes 1$, $e_i \otimes 1$ $(i \neq i_0)$, and $1 \otimes e_i$ $(i \neq i_0)$ are F-linearly independent in $A \otimes_F A$, so upon expanding the two sides of the identity $a \otimes 1 = 1 \otimes a$ we conclude that $c_i = 0$ for all $i \neq i_0$. Hence, $a = c_{i_0} e_{i_0} = c_{i_0} \in F$.

Now we drop the linear disjointness assumption but we assume that one of L or L' is Galois over F and that $L \cap L' = F$ inside of M. We wish to prove that $L \otimes_F L'$ is a field. By relabelling, assume L is Galois over F. By the primitive element theorem, $L = F(\alpha)$ for α with minimal separable polynomial $f \in F[T]$, so $L \simeq F[T]/(f)$ over F. Thus, $L \otimes_F L' \simeq L'[T]/(f)$. We need to prove that f is irreducible over L'. Let $h \in L'[T]$ be a monic factor of f with positive degree. Since $f \in M[T]$ splits with all roots in L, the same holds for h. In particular, all coefficients of $h \in M[T]$ lie in L. However, $h \in L'[T]$. Hence, since $L \cap L' = F$ we conclude that $h \in F[T]$, so by irreducibility of $f \in F[T]$ we must have $h = f$. ■

In general, if L and L' are finite extensions of F and are linearly disjoint over F, we shall write LL' to denote $L \otimes_F L'$. This is not too dangerous, in view of the preceding results.

Theorem 2.4. *If L and L' are finite Galois over F and are linearly disjoint over F, then LL' is Galois over F and the natural map*

$$\psi : \mathrm{Gal}(LL'/F) \to \mathrm{Gal}(L/F) \times \mathrm{Gal}(L'/F)$$

is an isomorphism.

Proof. Since LL' is a field that is a compositum of subfields that are Galois over F, it is Galois over F. If $\sigma \in \mathrm{Gal}(L'/F)$ and $\sigma' \in \mathrm{Gal}(L'/F)$ are two elements, then $\sigma \otimes \sigma'$ is an automorphism of $LL' = L \otimes_F L'$ over

F, and it is composite of commuting automorphisms $\sigma \otimes 1$ and $1 \otimes \sigma'$. Hence, this defines a map of groups

$$\widetilde{\psi} : \mathrm{Gal}(L/F) \times \mathrm{Gal}(L'/F) \to \mathrm{Gal}(LL'/F).$$

This is clearly an inverse to ψ. ■