Math 154. Application of ideal discriminant to unramifiedness

1. Motivation

Let A be a Dedekind domain with fraction field F, and let A' be the integral closure of A in a finite separable extension field F'/F, so A' is module-finite over A and is itself Dedekind (with fraction field F'). In class we defined the nonzero ideal $\mathrm{disc}(A'/A) \subset A$ whose prime factors are exactly those maximal ideals $\mathfrak{m}$ of A that are ramified in F'/F (i.e., for *some* prime factor $\mathfrak{m}'$ of $\mathfrak{m}A'$, either $\mathfrak{m}'$ occurs with multiplicity $e(\mathfrak{m}'|\mathfrak{m}) > 1$ or the residue field extension $A/\mathfrak{m} \to A'/\mathfrak{m}'$ is not separable).

In this handout, we use discriminant ideals to prove a very useful property of unramifiedness relative to composite fields. The setup is as follows. We suppose given to us two intermediate fields $F_1, F_2 \subset F'$ over F with composite field $F_1F_2 = F'$ (so each F_i/F is finite separable), and let $A_i \subset F_i$ be the integral closure of A in F_i, so A_i is module-finite over A and is Dedekind with fraction field F_i. Observe that the subring

$$A_1A_2 = \left\{ \sum_i x_{i,1}y_{i,2} \,|\, x_{i,1} \in A_1, y_{i,2} \in A_2 \right\}$$

generated by A_1 and A_2 inside F' is contained in A'; its fraction field contains $F_1F_2 = F'$ and thus is equal to F'. It is natural to ask: when does $A_1A_2 = A'$?

We known an affirmative answer in a special case: if $A = \mathbf{Z}$ (so $F = \mathbf{Q}$) and if

$$[F' : F] = [F_1 : F][F_2 : F]$$

then provided that the nonzero ideals $\mathrm{disc}(A_1/A)$ and $\mathrm{disc}(A_2/A)$ in $\mathbf{Z}$ have no nontrivial common factor we proved that $A' = A_1A_2$ and

$$\mathrm{disc}(A'/A) = \mathrm{disc}(A_1/A)^{[F_2:F]}\mathrm{disc}(A_2/A)^{[F_1:F]}.$$

(This was an ingredient in our determination of rings of integers of general cyclotomic fields.)

But the hypothesis $[F' : F] = [F_1 : F][F_2 : F]$ is *very restrictive*; e.g., if F'/F is a Galois extension with Galois group S_3 then it is generated by a pair of subfields of degree 3 over F, but the preceding cannot be applied in such situations. The aim of this handout is to prove that $A_1A_2 = A$ assuming coprimality of discriminant ideals $\mathrm{disc}(A_i/A)$ but *not* assuming anything about field degrees over F, and to give an applications to how the property of unramifiedness behaves under the formation of composite fields (again avoiding any assumptions on field degrees over F).

2. Some general lemmas

For any A-submodule N of F', let $N_{\mathfrak{m}}$ denote the set of fractions n/s for $n \in N$ and $s \in A - \mathfrak{m}$; this is clearly an $A_{\mathfrak{m}}$-submodule of F'.

Lemma 2.1. *Let $N \subset M$ be a containment of A-submodules of F'. If $N_{\mathfrak{m}} = M_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of A then $N = M$.*

Moreover, the natural $A/\mathfrak{m}$-linear map $N/\mathfrak{m}N \to N_{\mathfrak{m}}/\mathfrak{m}N_{\mathfrak{m}}$ is an isomorphism.

Proof. For the first assertion, we pick $m \in M$ and want to show that $m \in N$. Let J be the set of elements $a \in A$ such that $am \in N$. Clearly $0 \in J$, and one checks without difficulty (do it!) that J is an ideal of A. We want to show that $1 \in J$, or in other words that $J = A$. We assume to the contrary and seek a contradiction.

Assuming $J \neq A$, so J is a proper ideal of A, by the noetherian property of A we know that J is contained in a maximal ideal $\mathfrak{m}$ of A. By hypothesis $N_{\mathfrak{m}} = M_{\mathfrak{m}}$, so $m = n/s$ for some $n \in N$ and

$s \in A - \mathfrak{m}$. Hence, $sm = n \in N$, so $s \in J$. But $J \subset \mathfrak{m}$ by design, so $s \in \mathfrak{m}$, contradicting that $s \in A - \mathfrak{m}$!

To show that the natural map $f : N/\mathfrak{m}N \to N_{\mathfrak{m}}/\mathfrak{m}N_{\mathfrak{m}}$ is bijection, the key point is that we know $A/\mathfrak{m} \to A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$ is an isomorphism (i.e., the residue field at a maximal ideal of a domain is unaffected by first localizing at that maximal ideal). In particular, for any $s \in A - \mathfrak{m}$, the residue class $1/s \bmod \mathfrak{m}A_{\mathfrak{m}}$ in $A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$ is hit by some $a \in A$, which is to say $a = 1/s + b$ for some $b \in \mathfrak{m}A_{\mathfrak{m}}$. (This has a very concrete explanation: since $A/\mathfrak{m}$ is a field in which the image of s is nonzero, it admits a multiplicative inverse, which is to say we find $a \in A$ such that $as \equiv 1 \bmod \mathfrak{m}$ or equivalently $as = 1 + x$ for some $x \in \mathfrak{m}$, so $a = 1/s + b$ for $b := x/s \in \mathfrak{m}A_{\mathfrak{m}}$.) The surjectivity of f then follows: if $n \in N$ and $s \in A - \mathfrak{m}$ then $f(an \bmod \mathfrak{m}N) = n/s \bmod \mathfrak{m}N_{\mathfrak{m}}$ since $an - n/s = (a - 1/s)n = bn \in \mathfrak{m}N_{\mathfrak{m}}$ due to b belonging to $\mathfrak{m}A_{\mathfrak{m}}$.

It remains to show f is injective, which is to say that $\ker f = 0$. If $n \in N$ represents a class in $\ker f$ then n viewed inside $N_{\mathfrak{m}}$ belongs to $\mathfrak{m}N_{\mathfrak{m}}$, so via a common denominator in $A - \mathfrak{m}$ we have $n = n'/s$ for some $n' \in \mathfrak{m}N$ and $s \in A - \mathfrak{m}$. Hence, $sn = n' \in \mathfrak{m}N$, so the residue class $\overline{n} = n \bmod \mathfrak{m}N$ in $N/\mathfrak{m}N$ is killed by s. Our aim is to show $\overline{n} = 0$, so it suffices to show that s acts invertible on $N/\mathfrak{m}N$. But $N/\mathfrak{m}N$ as an A-module is really a vector space over the residue field $A/\mathfrak{m}$, and the element $s \in A - \mathfrak{m}$ has nonzero image in that residue field! Thus, s acts invertibly on any $A/\mathfrak{m}$-vector space (such as $N/\mathfrak{m}N$). ■

Keeping in mind our aim to show (under suitable hypotheses) that the inclusion of A_2-algebras $A_1A_2 \subset A'$ with the same fraction field F' is an equality, the following provides a useful sufficient criterion in terms of properties that will be inferred from the coprimality of the ideals $\operatorname{disc}(A_i/A)$.

Lemma 2.2. *Let $B \to B'$ be a module-finite extension of Dedekind domains inducing a finite separable extension of fraction fields $K \to K'$. Let $R \subset B'$ be a B-subalgebra with fraction field K'.*

Assume that for every maximal ideal $\mathfrak{n}$ of B and its associated residue field $k = B/\mathfrak{n}$, the k-algebra $R/\mathfrak{n}R$ is a product of separable finite extensions of k. Then $R = B'$ and $\operatorname{disc}(B'/B) = B$.

Proof. By Lemma 2.1, to show $R = B'$ it suffices to show that for every maximal ideal $\mathfrak{n}$ of B, the inclusion $R_{\mathfrak{n}} \subset B'_{\mathfrak{n}}$ of $B_{\mathfrak{n}}$-algebras is an equality. Likewise, to verify that the inclusion of ideals $\operatorname{disc}(B'/B) \subset B$ is an equality it suffices to check after localizing at each maximal ideal of B (such localization commutes with the formation of the discriminant).

Exactly as in the preceding lemma (now using B in the role of A there), the natural map $R/\mathfrak{n}R \to R_{\mathfrak{n}}/\mathfrak{n}R_{\mathfrak{n}}$ of $B/\mathfrak{n}$-algebras is an isomorphism. Thus, we may localize throughout at $\mathfrak{n}$ (i.e., invert $B - \mathfrak{n}$) to reduce to the case when B is a discrete valuation ring with unique maximal ideal $\mathfrak{n}$. Hence, B is a PID, so R and B' are free of finite rank as B-modules. Their B-ranks coincide with the degree n of K' over K (since we know that localizing each at $B - \{0\}$ recovers the common fraction field of each and thereby identifies a B-basis of R or B' with a K-basis of K').

We don't yet know if the B-algebra R with fraction field K' is Dedekind, but it is B-free and the element $\det(\operatorname{Tr}_{K'/K}(r_ir_j)) \in B$ for any B-basis $\{r_i\}$ is nonzero and changes by a unit square of B under a change of B-basis (by the same purely linear-algebraic reasoning used in the classical setting with $B = \mathbf{Z}$), so the nonzero ideal it generates in R is independent of the B-basis $\{r_i\}$; it is denoted $\operatorname{disc}(R/B)$. The structure theorem for torsion-free finitely generated modules over a PID provides ordered B-bases $\{e_1, \dots, e_n\}$ of R and $\{e'_1, \dots, e'_n\}$ of B' with $e_i = b_ie'_i$ for some nonzero $b_1, \dots, b_n \in B$. Thus, the quotient B'/R as a B-module is $\prod(B/(b_i))$. We will prove $b_i \in B^{\times}$ for all i, so $R = B'$ as desired.

Exactly as in the classical setup with integer rings over $\mathbf{Z}$ and subrings of finite index, a matrix calculation with the trace pairings $\mathrm{Tr}_{K'/K}(e_ie_j)$ and $\mathrm{Tr}_{K'/K}(e'_ie'_j)$ gives the equality

$$\mathrm{disc}(R/B) = \mathrm{disc}(B'/B)\prod(b_i)^2$$

as nonzero principal ideals of B. Thus, to show that all b_i's are units in B it suffices to show that the nonzero ideal $\mathrm{disc}(R/B)$ in the Dedekind domain B has no prime factor occurring with multiplicity at least 2. Even better, we will show that $\mathrm{disc}(R/B) = B$. More specifically, we claim that the element

$$\delta := \det(\mathrm{Tr}_{K'/K}(e_ie_j))$$

in the dvr B is a unit, or equivalently has nonzero image in the residue field $k = B/\mathfrak{n}$.

By the module-freeness of R over B, we can make sense of $\mathrm{Tr}_{R/B} : R \to B$ as a B-linear map coinciding with the restriction to R of $\mathrm{Tr}_{K'/K}$ (by recognizing that a B-basis of R is also a K-basis of $(B-\{0\})^{-1}R = \mathrm{Frac}(R) = K'$). That is, by definition $\mathrm{Tr}_{R/B}(r)$ is the trace of the matrix of the B-linear multiplication on R by r. Thinking in terms of matrix traces,

$$\mathrm{Tr}_{R/B}(r) \bmod \mathfrak{n} = \mathrm{Tr}_{\overline{R}/k}(r \bmod \mathfrak{n})$$

for $\overline{R} := R/\mathfrak{n}R$, as in our proof that prime factors of $\mathrm{disc}(\mathscr{O}_E/\mathbf{Z})$ are precisely the primes ramified in a number field E. Thus,

$$\delta \bmod \mathfrak{n} = \det(\mathrm{Tr}_{\overline{R}/k}(\overline{e}_i\overline{e}_j))$$

in k, where the reductions $\overline{e}_i := e_i \bmod \mathfrak{n}R$ constitute a k-basis of $\overline{R}$.

The upshot is that $\delta \bmod \mathfrak{n} = \mathrm{disc}(\overline{R}/k)$ in k (up to $(k^\times)^2$-multipliers), so it suffices to show that this latter discriminant in k is nonzero. But recall that by hypothesis, as a k-algebra $\overline{R} = \prod k_i$ for some finite separable extensions k_i of k. By consideration of block matrices relative to a basis adapted to a direct product decomposition of rings, over any field the discriminant of a direct product of two finite-dimensional algebras is the product of the discriminants (up to nonzero square multiple). Thus, $\delta \bmod \mathfrak{n} = \prod \mathrm{disc}(k_i/k)$ up to $(k^\times)^2$-multiple. But each k_i is a *separable* finite extension of k, whence its discriminant over k is nonzero. ■

We require one final lemma before taking up the proof of the main result.

Lemma 2.3. *For any fields $E_1, \dots, E_m$, the ideals of the ring $R := \prod_{j=1}^m E_j$ are precisely*

$$I_J = \prod_{j\in J} E_j \times \prod_{i\notin J}\{0\}$$

for subsets $J \subset \{1, \dots, m\}$. In particular, every nonzero quotient ring of R has the form $R/I_J = \prod_{i\notin J} E_i$ viewed as a quotient via projection onto the factor fields indexed by $\{1, \dots, m\} - J$ for a proper subset $J \subset \{1, \dots, m\}$.

Proof. Let $e_j \in R$ be the element whose jth component is 1 and whose other components vanish, so $\sum e_j = 1$. For any $r \in R$ we have $r = r\cdot 1 = r\cdot(\sum e_j) = \sum re_j$, with re_j having vanishing component away from the jth. Since an ideal that contains r must contain each multiple re_j of r, every ideal I of R is generated by elements that vanish away from at most one factor.

If a nonzero element r of R has vanishing component away from the jth factor then its jth component is given by some $c_j \in E_j^\times$, so $r = ue_j$ for the unit $u \in R^\times$ whose jth component is c_j and whose other components are all equal to 1. Hence, an ideal contains such an r if and only if it contains e_j. The upshot is that every ideal of R is generated by some e_j's. For a subset $J \subset \{1, \dots, m\}$, the ideal generated by $\{e_j\}_{j\in J}$ is I_J. ■

3. Integral closure in a composite field

Here is the main result we want to prove:

Theorem 3.1. *Let F'/F be a finite separable extension and let $F_1, F_2 \subset F'$ be subextensions over F whose compositum is equal to F'. Let $A_i \subset F_i$ be the integral closure of A, and assume the nonzero ideals $\mathrm{disc}(A_1/A)$ and $\mathrm{disc}(A_2/A)$ of the Dedekind domain A have no common prime factor. Then the integral closure $A' \subset F'$ of A is equal to A_1A_2.*

With more advanced techniques in commutative algebra (e.g., tensor products or completions), this proof can be streamlined considerably. The proof below was made by starting with a very short proof based on more sophisticated methods and modifying the argument to avoid the need for such methods; this might make the argument look more magical than it really is.

Proof. The formation of the integral closures A_1, A_2, and A', as well as of the A-subalgebra A_1A_2 inside F', is compatible with localizing at any multiplicative subset of $A - \{0\}$. The formation of discriminant ideals $\mathrm{disc}(A_i/A)$ also commutes with such localization, and the hypothesis that they share no nontrivial common factor is preserved after such localization. Thus, by Lemma 2.1 (applied with $N = A_1A_2$ and $M = A'$), for our desired conclusion we may localize throughout at an arbitrary maximal ideal $\mathfrak{m}$ of A (i.e., invert $A - \mathfrak{m}$) to reduce to checking the desired result when A is a discrete valuation ring.

Now there is only one maximal ideal $\mathfrak{m}$ in A. This maximal ideal cannot divide both discriminant ideals $\mathrm{disc}(A_i/A)$ by our hypotheses, so at least one of these ideals in the dvr A is the unit ideal. Swapping labels if necessary, we may assume $\mathrm{disc}(A_1/A) = A$. In other words, F_1/F is unramified at the unique maximal ideal $\mathfrak{m}$ of A. This says

$$\mathfrak{m}A_1 = \prod_{i=1}^{g} \mathfrak{m}_i$$

for maximal ideals $\mathfrak{m}_i$ of A_1 such that each residue field $\kappa_i = A_1/\mathfrak{m}_i$ is separable (of finite degree) over $\kappa := A/\mathfrak{m}$. Hence, the Chinese Remainder Theorem for Dedekind domains (applied to A_1) gives

$$\overline{A}_1 := A_1/\mathfrak{m}A_1 \simeq \prod_{i=1}^{g} \kappa_i$$

as κ-algebras. The primitive element theorem provides a nonzero primitive element c_i for κ_i/κ, so $\kappa_i = \kappa(c_i) \simeq \kappa[X]/(f_i)$ for the separable irreducible minimal polynomial $f_i \in \kappa[X]$ of c_i over κ (so $f_i(0) \in \kappa^\times$ since $c_i \neq 0$). Let $\xi_i \in \overline{A}_1$ be the element given by $c_i \in \kappa_i^\times$ in the ith component κ_i and 0 in all other factor fields, so the ξ_i's generate $\overline{A}_i$ as a κ-algebra (why?). Note that $e_i := f_i(0)^{-1}(f_i(\xi_i) - f_i(0))$ is the element over $\overline{A}_1 = \kappa_1 \times \cdots \times \kappa_g$ whose ith component is 1 and whose other components vanish, so $e_i^2 = e_i$, $e_ie_{i'} = 0$ when $i' \neq i$, and $\sum e_i = 1$. (These properties of the e_i's are expressed by saying that they are pairwise orthogonal idempotents that sum to 1.) Note also that $\xi_ie_i = \xi_i$ and $f_i(\xi_i)e_i = 0$ for all i.

By Lemma 2.2 applied with $B = A_2$, $R = A_1A_2$, and $B' = A'$, it suffices to show that for every maximal ideal $\mathfrak{n}$ of A_2, $\overline{R} := R/\mathfrak{n}R$ is a product of finite separable extensions of $k = A_2/\mathfrak{n}$. (Note that $\overline{R}$ is nonzero, which is to say that 1 is not an R-linear combination of elements of $\mathfrak{n}$ since even $\mathfrak{n}A' \neq A'$ by our work with module-finite extensions of Dedekind domains applied to $A_2 \to A'$.) Since the maximal ideal $\mathfrak{n}$ of A_2 lies over the unique maximal ideal $\mathfrak{m}$ of A (with $A/\mathfrak{m} =: \kappa$), so $\mathfrak{m} \subset \mathfrak{n}$, the inclusion of rings $A_1 \subset R$ induces a natural κ-algebra map

$$h : \overline{A}_1 = A_1/\mathfrak{m}A_1 \to R/\mathfrak{n}R =: \overline{R}.$$

Since $k := A_2/\mathfrak{n}$ and $R := A_1A_2$ consists of A_1-linear combinations of elements of A_2, every element of $\overline{R}$ is a k-linear combination of elements of $h(\overline{A}_1)$. But $\overline{A}_1$ is generated by the ξ_i's as a κ-algebra, so $\overline{R}$ is generated as a k-algebra by the elements $h(\xi_i)$. Moreover, since h is a ring homomorphism, the elements $\varepsilon_i := h(e_i)$ in $\overline{R}$ inherit the properties of the e_i's in $\overline{A}_1$: $\varepsilon_i^2 = \varepsilon_i$, $\varepsilon_i\varepsilon_{i'} = 0$ whenever $i' \neq i$, and $\sum_i \varepsilon_i = 1$ (i.e., the ε_i's are pairwise orthogonal idempotents that sum to 1).

Consider the k-linear map

$$q : k[Y_1] \times \cdots \times k[Y_g] \to \overline{R}$$

defined by $(p_1(Y_1), \dots, p_g(Y_g)) \mapsto \sum p_i(h(\xi_i))\varepsilon_i$. The properties of the ε_i's imply that q is a *ring homomorphism* (check!), so q is a k-algebra homomorphism. But the g-tuple whose ith component is Y_i and whose other components vanish is carried by q onto $\xi_i\varepsilon_i = \xi_i$, and we have seen that the ξ_i's generate $\overline{R}$ as a k-algebra, so q is *surjective*. Moreover, q kills any g-tuple $(p_1, \dots, p_g)$ for which $f_i|p_i$ for all i since the κ-algebra homomorphism property of h ensures that

$$f_i(h(\xi_i))\varepsilon_i = h(f_i(\xi_i))h(e_i) = h(f_i(\xi_i)e_i) = h(0) = 0.$$

Thus, q factors (uniquely) through a well-defined k-algebra map

$$\overline{q} : k[Y_1]/(f_1(Y_1)) \times \cdots \times k[Y_g]/(f_g(Y_g)) \to \overline{R}$$

that must be surjective.

In other words, $\overline{R}$ is a quotient of the product of the k-algebras $k[Y_i]/(f_i(Y_i))$. But f_i is separable over k since by design it is a separable polynomial over the subfield $\kappa \subset k$, so the Chinese Remainder Theorem ensures that the k-algebra $k[Y_i]/(f_i(Y_i))$ is a direct product of finite separable extesions of k (corresponding to the irreducible monic factors of f_i over k). Hence, $\overline{R}$ is a quotient of a direct product of finite separable extensions of k, so $\overline{R}$ itself is such a product by Lemma 2.3! ■

4. Unramifiedness in composite fields

As an application of Theorem 3.1 (and of a technique in its proof), we can establish good behavior of unramifiedness when forming composite fields. Consider a compositum $F' = F_1F_2$ over $F = \mathrm{Frac}(A)$ and the associated integral closures A_1, A_2, A' as at the outset.

By using localization at maximal ideals, our earlier techniques over $\mathbf{Z}$ adapt without change to prove that if the degrees $d_i = [F_i : F]$ have product equal to $[F' : F]$ then

$$\mathrm{disc}(A'/A) = \mathrm{disc}(A_1/A)^{d_2}\mathrm{disc}(A_2/A)^{d_1}.$$

Thus, in such cases a maximal ideal $\mathfrak{m}$ of A is unramified in F_1 and F_2 (equivalently, it doesn't divide either of the ideals $\mathrm{disc}(A_i/A)$) if and only if it is unramified in $F' = F_1F_2$ (equivalently, it doesn't divide $\mathrm{disc}(A'/A)$).

Our aim is to show that this equivalence of unramifiedness properties is valid *without* any hypotheses relating the F-degrees of F_1, F_2, F'. In the absence of such F-degree hypotheses there is *no* simple formula relating $\mathrm{disc}(A_1/A)$, $\mathrm{disc}(A_2/A)$, and $\mathrm{disc}(A'/A)$. Nonetheless, we shall prove that $\mathfrak{m}$ divides $\mathrm{disc}(A'/A)$ if and only if it divides at least one of the $\mathrm{disc}(A_i/A)$'s:

Proposition 4.1. *A maximal ideal $\mathfrak{m}$ of A is unramified in F'/F if and only if it is unramified in both F_1/F and F_2/F.*

Proof. The implication "⇒" is a consequence of the elementary behavior of of prime ideal factorization and separability in towers, as follows. Since $\mathfrak{m}A' = (\mathfrak{m}A_i)A'$, if some $\mathfrak{m}A_i$ has a prime factor $\mathfrak{n}$ appearing with multiplicity $e > 1$ then $\mathfrak{m}A'$ is divisible by $(\mathfrak{n}A')^e$ and hence any prime of A' over $\mathfrak{n}$ (at least one of which does exist!) occurs in $\mathfrak{m}A'$ with multiplicity that is a positive integral multiple of e and hence is > 1. That would contradict that $\mathfrak{m}A'$ is assumed to have no repeated prime factors. Likewise, suppose some prime factor $\mathfrak{m}_i$ of $\mathfrak{m}A_i$ for some $i \in \{1,2\}$ has associated residue field $A_i/\mathfrak{m}_i$ that is *not* separable over $A/\mathfrak{m}$. Pick a prime $\mathfrak{m}'$ of A' over $\mathfrak{m}_i$ (as does exist!); this is also a prime factor of $\mathfrak{m}A'$. The residue field extension

$$A/\mathfrak{m} \to A'/\mathfrak{m}'$$

has subextension $A_i/\mathfrak{m}_i$ that is not separable over $A/\mathfrak{m}$, so $A'/\mathfrak{m}'$ cannot be separable over $A/\mathfrak{m}$ either, contradicting the assumption of unramifiedness for $\mathfrak{m}$ in F'.

Now we turn to the harder converse implication: assuming $\mathfrak{m}$ is unramified in each F_i we claim the same for F'. It is harmless to first localize at $\mathfrak{m}$, so A is a dvr with $\mathfrak{m}$ as its unique maximal ideal. The unramifiedness hypothesis implies that the nonzero ideals $\mathrm{disc}(A_i/A)$ in the dvr A are not divisible by $\mathfrak{m}$, so the only option is that these each coincide with the unit ideal A. For each maximal ideal $\mathfrak{m}'$ of A', so $\mathfrak{m}'$ lies over the unique maximal ideal $\mathfrak{m}$ of A (equivalently, $\mathfrak{m}'$ is a prime factor of $\mathfrak{m}A'$), we seek to show that $\mathfrak{m}'$ occurs with multiplicity 1 in the factorization of $\mathfrak{m}A'$ and that the extension of residue fields

$$A/\mathfrak{m} \to A'/\mathfrak{m}'$$

is separable.

The ideal $\mathfrak{n} = \mathfrak{m}' \cap A_2$ of A_2 is maximal and contains $\mathfrak{m}$, so by the unramifiedness of $\mathfrak{m}$ in F_2 we know that $\mathfrak{n}$ occurs once in the prime factorization of $\mathfrak{m}A_2$ and that $A_2/\mathfrak{n}$ is separable over $A/\mathfrak{m}$. Since $\mathfrak{m}A_2$ is a product of distinct primes $\mathfrak{n}_j$ (including $\mathfrak{n}$) with multiplicity 1, the prime factorization of $\mathfrak{m}A' = (\mathfrak{m}A_2)A'$ is the concatenation of the prime factorizations of each $\mathfrak{n}_jA'$. This concatenation process doesn't introduce any repetition of prime factors from two distinct j's since any prime factor of $\mathfrak{n}_jA'$ meets A_2 in exactly $\mathfrak{n}_j$ and so cannot also be a prime factor of $\mathfrak{n}_{j'}A'$ for some $j' \neq j$.) Hence, to show that $\mathfrak{m}'$ appears with multiplicity 1 in $\mathfrak{m}A'$ it suffices to show that each $\mathfrak{n}_j$ is unramified in F'/F_2. Likewise, by considering the tower of residue field extensions

$$A/\mathfrak{m} \to A_2/\mathfrak{n} \to A'/\mathfrak{m}'$$

whose bottom layer is separable, to show that the entire extension is separable it suffices to check for the top layer (as separability is transitive in finite extensions of fields).

To summarize, our task is reduced to showing that F'/F_2 is unramified at *all* maximal ideals of A_2, which is to say that $\mathrm{disc}(A'/A_2) = A_2$. Now we pull out the big guns: by Theorem 3.1 we have $A' = A_1A_2$ since each $\mathrm{disc}(A_i/A)$ is equal to A (ensuring that these ideals are certainly relatively prime). But in the proof of Theorem 3.1 we showed that for any maximal ideal $\mathfrak{n}$ of A_2, the quotient ring $A'/\mathfrak{n}A' = (A_1A_2)/\mathfrak{n}(A_1A_2)$ as an algebra over the residue field $k := A_2/\mathfrak{n}$ is a direct product of finite separable extensions of k. This holds for all $\mathfrak{n}$, so by Lemma 2.2 (with $B = A_2$ and $R = B' = A'$) gives that $\mathrm{disc}(A'/A_2) = A_2$ as desired. ■