Supplementary field theory notes

E/F is a finite field extension throughout. We also fix an algebraic closure $\overline{F}$ in which all our extensions live, although it will rarely be explicitly mentioned. Further extensions such as composites, split closures, etc., are then formed within $\overline{F}$. Alternatively one could work in some finite extension big enough to contain all the fields under consideration.

I always picture diagrams of field extensions vertically, with F at the bottom. For example, if K_1, K_2 are intermediate extensions I would put the picture in a "diamond" with F at the bottom. But I am too lazy to do this in Tex so I will leave it to you to draw the diagrams, which are, I claim, indispensable for visualizing what's going on.

1 Separability and splitting fields

1.1 Splitting fields

Let's begin with a conceptually clearer definition of a splitting field. We say that E/F is a *splitting field over* F if every irreducible $f \in F[x]$ with a root in E splits in E. Now contrast this with the definition of "splitting field E/F of a polynomial $f \in F[x]$": This means that f splits in E and E is the minimal such field, i.e., E is generated by the roots of f. Some authors then define "splitting field" to mean that E/F is the splitting field of some f. Recall that we showed these two definitions agree:

Proposition 1.1 *E/F is a splitting field if and only if it is the splitting field of some $f \in F[x]$ (equivalently, E contains and is generated by the complete set of roots of some polynomial).*

Recall also that the "only if" is easy, whereas the "if" is not at all obvious—it says that by adjoining all the roots of this one polynomial f, by magic *every* polynomial with a root in E splits in E. The proof used our theorems about extending isomorphisms or more generally monomorphisms of fields.

I remark also that instead of the "splitting field of a polynomial" it would make more sense to talk about the splitting field of a set of polynomials, defined in the obvious way. In particular, by allowing the set in question to be infinite, one can easily modify the proposition so that it holds for infinite-dimensional algebraic extensions. But even in the finite case, it's convenient to define the splitting field E of a finite set $S = \{f_1, ..., f_n\}$ of polynomials in the aforementioned obvious way: E is the smallest field containing all the roots of the f_i's. Now, it's certainly true that this is the same thing as taking the splitting field of the product $f := f_1...f_n$, but personally I find that this insistence on a single polynomial can be distracting. Sometimes it's convenient to give a splitting field as the splitting field of a finite set of *irreducible* polynomials.

Similarly, the most natural definition of the *split closure* of E/F is that is the field $\tilde{E}$ obtained by adjoining all the roots of every irreducible $f \in F[x]$ that has a root in E. It is then immediate that $\tilde{E}$ is the unique minimal splitting field containing E. On the face of it, it might seem possible that $\tilde{E}$ is infinite-dimensional, but we know this ain't so; indeed the following is immediate from the previous proposition:

Proposition 1.2 *Suppose $\alpha_1, ..., \alpha_m$ generate E/F. Then $\tilde{E}$ is the splitting field of $\{f_{\alpha_1}, ..., f_{\alpha_m}\}$.*

Let $G = G(\tilde{E}/F)$. Note we are not assuming E is separable over F, so $\tilde{E}$ need not be a Galois extension. But the Galois group is still perfectly well-defined, as the F-automorphism of $\tilde{E}$. We may then characterize $\tilde{E}$ as follows:

Proposition 1.3 *$\tilde{E}$ is the composite of the subextensions σE, $\sigma \in G$. (In fact it suffices to take σ ranging over a set of coset representatives for $G/G(\tilde{E}/E)$.)*

Proof: This is clear, since if an irreducible f has a root $\alpha \in E$, then every root lies in one of the σE's.

We'll call a subfield of the form σE as above a *Galois translate* of E. Then the proposition says that L is the composite of the Galois translates of E.

Finally, we note:

Proposition 1.4 *Split closure commutes with composites: $\widetilde{K_1 K_2} = \tilde{K}_1 \tilde{K}_2$.*

Proof: Note that $\tilde{K}_1 \tilde{K}_2$ is a splitting field over F, contains $K_1 K_2$, and is contained in $\widetilde{K_1 K_2}$. By definition of split closure, this last containment is an equality.

1.2 Separable extensions

An element $\alpha \in E$ is *separable* if its irreducible (a.k.a. "minimal") polynomial f_α is separable, i.e. has no repeated roots. In this form the definition makes sense for any algebraic extension, finite or not. Notice, however, that we run into a problem similar to the one we encountered for splitting fields. If E/F is merely generated by separable elements, is it a separable extension? This isn't obvious even for simple extensions. Fortunately, there is an analogue of Proposition 1.1, although its interesting proof is significantly harder. The key theorem is the case where we also have splitting fields, and Galois theory can be applied. Before stating it, recall we have already shown that E/F is Galois if and only if it is a separable splitting field.

Theorem 1.5 *E/F is a separable splitting field if and only if it is the splitting field of a separable polynomial (or finite set of irreducible separable polynomials).*

Here again the "only if" is easy (we'll omit the proof), whereas the "if" is highly non-obvious. It says that after adjoining the roots of a single separable polynomial, presto!—every element in the resulting field extension is separable.

Proof: Suppose E is the splitting field of the separable irreducible polynomials $f_1, ..., f_m$. To show E/F is separable, it suffices to show it is Galois. Thus if $G = G(E/F)$, we want to show $E^G = F$. By Artin's theorem E/E^G is Galois with Galois group G, and $[E : E^G] = |G|$. So it is enough to show $[E : F] = |G|$.

Let $\alpha \in E$ be a root of f_1, with $deg\, f_1 = d > 1$. Then $E/F(\alpha)$ is the splitting field of a set of separable irreducible polynomials, namely the irreducible factors in $F(\alpha)[x]$ of the f_i's. So by induction on $[E : F]$ we can assume that $E/F(\alpha)$ is Galois. Let $H = G(E/F(\alpha))$, so $|H| = [E : F(\alpha)]$. I claim that $[F(\alpha) : F] = [G : H]$. Granting this, we have

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] = |H| \cdot [G : H] = |G|$$

and we're done. To prove the claim, recall that G acts transitively on the set R of roots of f_1. (There is no circularity here, as the transitivity does not require that E/F Galois but only that it is a splitting field.) The isotropy group of α for this action is none other than H. Hence

$$[F(\alpha) : F] = d = |R| = [G : H],$$

where the middle equality holds because f_1 is separable and so has d distinct roots. QED!

As a corollary we get something more analogous to Proposition 1.1.

Corollary 1.6 *E/F is separable if and only if it is generated by separable elements (we can always take the generating set to be finite, since we're assuming E/F is finite).*

Proof: Suppose E/F is generated by separable elements $\alpha_1, ..., \alpha_m$. Then $\tilde{E}$ is the splitting field of the separable polynomials f_{α_i}, so by the theorem $\tilde{E}/F$ is separable. But clearly any subextension of a separable extension is separable.

Corollary 1.7 *The set S of elements of E that are separable over F form a subfield, and hence a subextension of E/F.*

Proof: Suppose $\alpha, \beta \in E$ are separable. Then $F(\alpha), F(\beta)$ are separable over F, and by the previous corollary $F(\alpha, \beta)$ is also separable over F. Hence S is closed under sums, products and inverses (although in a finite extension there is no need to check inverses separately, since every finite-dimensional integral domain is a field).

Note that S is the unique maximal separable subextension of E/F, called the *separable closure* of F in E. If F is perfect then of course $S = E$, whereas in our standard example with $F = \mathbb{F}_p(t)$, $E = F(\sqrt[p]{t})$, we have $S = F$. It isn't hard to cook up examples in which S lies strictly between F and E.

2 Properties of extensions

In this section we consider systematically to what extent the properties such as "separable", "splitting field" and so on are preserved or inherited by intermediate fields, composites, intersections, etc. The discussion will automatically answer the same question for "Galois", since E/F is Galois if and only if it is a separable splitting field. It is very much worthwhile to do this systematically, in order to streamline later arguments and avoid repeating the same arguments over and over again. We assume throughout that the property P in question is

isomorphism invariant, in the sense that whenever $E \longrightarrow E'$ is an isomorphism of extensions of F, E has P if and only if E' has P. Particular emphasis goes to the following four conditions we might hope for in a property P.

Splicing. Let K be an intermediate field. We say that E/F is obtained by *splicing* the extensions K/F and E/K. A property P is preserved by splicing if whenever K/F and E/K have P, then E/F has P.

Base change. Consider two intermediate fields K_1, K_2. In this situation we call the extension K_1K_2/K_2 the *base change* of the extensions K_1/F, the idea being that we have changed the base field from F to K_2. We say that P is preserved by base change if whenever K_1/F has P, so does K_1K_2/K_2.

Composites. Again consider intermediate fields K_1, K_2. A property P is preserved by composites if whenever K_1/F, K_2/F have P, so does K_1K_2/F.

Split closure. P is preserved by split closure if whenever E/F has P, so does the split closure $\tilde{E}/F$.

Observation: If P is preserved by splicing and base change, then it is preserved by composites and split closures. The proof for composites is trivial (look at the diamond!). The split closure $\tilde{E}$ is the composite of the Galois translates of E, so by isomorphism invariance we conclude that P is also preserved by split closures. These observations reduce the workload considerably.

We now turn to some examples of P. The isomorphism invariance is obvious in all cases and we won't discuss it further.

Proposition 2.1 *a) The properties "splitting field" (meaning that E/F is a splitting field) and "Galois" are preserved by base change, composites and split closures (albeit the last item is silly, since then $\tilde{E} = E$), but not by splicing.*

b) The property "separable" is preserved by splicing, base change, composites and split closures.

Proof: a) That splitting fields are preserved by base change and composites is trivial from what we've already done. For example, suppose K_1/F is the splitting field of f; then K_1K_2/K_2 is again the splitting field of f, regarded as an element of $K_2[x]$. The composite case is similar. The corresponding statements for "Galois" then follow immediately from part (b) below, since Galois is equivalent to separable splitting field. For a simple counterexample to preservation under splicing, take $\mathbb{Q} \subset \mathbb{Q}\sqrt{2} \subset \mathbb{Q}\sqrt[4]{2}$.

b) It suffices to check preservation under splicing and base change. For base change, suppose K_1/F is separable, and let $\alpha_1, ..., \alpha_m$ be a generating set. Then these elements also generate K_1K_2/K_2, and moreover are separable over K_2: For if f_{α_i} has distinct roots, and g_i denotes the irreducible polynomial of α_i in K_1K_2/K_2, then g_i divides f_{α_i} in $K_2[x]$ and so has distinct roots. The preservation under splicing is more involved, and postponed to the section "Inseparable extensions" below.

Remark. Since Galois extensions are preserved by base change and composites, we can ask what group-theoretic properties are preserved. In the case of base change, $G(K_1K_2/K_2) \longrightarrow G(K_1/F)$ is injective, so any property inherited by subgroups is preserved: cyclic, abelian, solvable, etc. In the case of composites, $G(K_1K_2/F) \longrightarrow G(K_1/F) \times G(K_2/F)$ is injective, so any property inherited by subgroups and products is preserved: abelian, solvable, etc.

In connection with splicing, we can ask the "reverse" questions of whether a property P of E/F is inherited by K/F and/or E/K. For example, we know that "Galois" is inherited by E/K but not by K/F. But separability is inherited in both cases.

Proposition 2.2 *If E/F is separable, then so are K/F and E/K are separable (and so in fact we have a biconditional statement).*

Proof: Suppose E/F is separable; then certainly K/F is, as already noted in a previous proof. Now suppose $\alpha \in E$ is separable over F, i.e. its irreducible polynomial f_α has distinct roots. Let $f_\alpha = f_1 ... f_k$ be a factorization into irreducibles in $K[x]$. One of the factors, say f_1, is the irreducible polynomial of α over K. Then since f_α has distinct roots, so does f_1, proving that E/K is separable.

Next we consider intersections.

Proposition 2.3 *Let K_1, K_2 be intermediate fields. Then if K_1 and K_2 are separable over F, so is $K_1 \cap K_2$, and similarly for "splitting field" and "Galois".*

Proof: The separable case is immediate, since any subextension of a separable extension is separable. Now suppose each K_i is a splitting field over F. Let $f \in F[x]$ be irreducible and have a root in $K_1 \cap K_2$; we must show f splits in $K_1 \cap K_2$. But it splits in each K_i separately, so all the roots lie in $K_1 \cap K_2$. The Galois case follows immediately.

3 Inseparable extensions

No such extensions exist in characteristic zero, so we assume throughout this section that F has prime characteristic p. We say that E/F is *purely inseparable* if the only elements separable over E are the elements of F, i.e. the separable closure of F in E is just F. Our standard example with the function field $F = \mathbb{F}_p(t)$ is an example of a purely inseparable extension. The good news is that such extensions are actually far simpler than a typical separable extension, and indeed are just mild generalizations of the standard example. To get started we have the elementary:

Lemma 3.1 *Let E/F be algebraic (of characteristic p), and let $\alpha \in E$. Then for some n, α^{p^n} is a separable element.*

Proof: If α is not separable, then by the derivative criterion we have $f'_\alpha = 0$. Hence f_α has the form $\sum a_i x^{pm_i}$. So α^p is a root of $\sum a_i x^{m_i}$, and indeed the latter is its irreducible

polynomial. Repeating the process with α replaced by α^p, and continuing, after a finite number of steps we arrive at an irreducible g with $g' \neq 0$ and $g(u^{p^n}) = 0$, QED.

Now call an element $\alpha \in E$ purely inseparable over F if its irreducible polynomial has the form $x^{p^n} - a$ for some $a \in F$. Note that such a polynomial has only one root.

Proposition 3.2 *The following are equivalent:*
a) E/F is purely inseparable;
b) every element of E is purely inseparable;
c) for every $\alpha \in E$, there is an n such that $\alpha^{p^n} \in F$.

Proof: (a) $\Rightarrow$ (c): Suppose E/F is purely inseparable, and $\alpha \in E$. Then α^{p^n} is separable over F for some n, hence $\alpha^{p^n} = b$ for some $b \in F$.

(c) $\Rightarrow$ (b): If $\alpha^{p^n} = b \in F$, then f_α divides $x^{p^n} - b$ and so over E has the form $(x-\alpha)^m$ for some m. For $1 < k < m$, $\alpha^k \notin F$ (otherwise there is a polynomial of degree $< m$ vanishing on α). Since the coefficient of x^k is $\pm\binom{m}{k}\alpha^k$ and lies in F, this forces $\binom{m}{k} = 0 \bmod p$ for all $1 < k < m$. The latter congruence holds if and only if m is a power of p (a mandatory exercise if you've never done it before!).

(b) $\Rightarrow$ (a): Clear, since $x^{p^n} - a$ is not separable unless $n = 0$.

Proposition 3.3 *a) The purely inseparable elements of E form a subextension P. It is the unique maximal purely inseparable extension.*
b) purely inseparables are closed under formation of composite fields;
c) If K is an intermediate field, then E/F is purely inseparable if and only if K/F and E/K are purely inseparable.
d) If E/F is purely inseparable then $[E : F] = p^n$ for some n.

Proof: a) Using condition (c) of the previous proposition, it is immediate that the purely inseparable elements are closed under addition and multiplication (and as usual in any algebraic extension, it isn't necessary to check multiplicative inverses).

b) In view of (a), this is immediate from the definition of the composite of two extensions.

c) Trivial from the definition.

d) This is true if the extension is simple, since α must be purely inseparable. The general case follows by induction on $[E : F]$ using (one part of) part (c).

Proposition 3.4 *Let S denote the separable closure of F in E. Then E is purely inseparable over S.*

Proof: Let $\alpha \in E$; then for some n we have α^{p^n} separable over F, and hence $\alpha^{p^n} \in S$. As seen earlier, this implies the irreducible polynomial of α has the form $x^{p^m} - a$ for $a \in S$, i.e. α is purely inseparable.

Finally, let's clear up some unfinished business from an earlier section.

Proposition 3.5 *If K is an intermediate field and K/F, E/K are separable, so is E/F.*

Proof: In fact this proposition was asserted for arbitrary fields F, but in characteristic zero there is nothing to prove. So we may keep our assumption $char\, F = p$. Let S be the separable closure of F in E; we must show $S = E$. Note $K \subset S$, since K/F is separable. Since E/K is separable, so is E/S by an earlier result. But E/S is also purely inseparable, forcing $S = E$.

Remark. We have seen that every extension E/F can be "factored" as separable extension followed by a purely inseparable extension, namely $F \subset S \subset E$. The natural question arises: Can we do it the other way, with the purely inseparable extension coming first and then the separable one? The obvious approach is to try to show that E is separable over P, the maximal purely inseparable subextension. But this doesn't work; nor does anything else: the answer to the question is "no". For a counterexample see Dummit and Foote, exercise 3 of §14.9.

4 Cyclic extensions

To get started on determining all finite Galois extensions of a field F (leaving it a bit vague what it means to "determine" them), a sensible plan is to start with the simplest case of cyclic extensions. Even here, we will give a complete answer only under some special assumptions. Let $n > 0$ satisfy (i) $char\, F$ doesn't divide n; and (ii) F contains the n-th roots of unity. In this case we get an elegant result:

Theorem 4.1 *Let $n > 0$ satisfy (i) $char\, F$ doesn't divide n; and (ii) F contains the n-th roots of unity.*

a) Suppose that $E = F(\alpha)$, where $\alpha^n = a \in F$. Then E/F is a cyclic Galois extension of degree d dividing n.

b) Suppose that E/F is cyclic of degree n. Then $E = F(\alpha)$ with $\alpha^n = a \in F$, and $x^n - a$ is irreducible.

Proof: a) This one is easy, and in fact we've more or less done it in earlier work. The point is that an element σ of the Galois group is determined by what it does to α, and clearly $\sigma(\alpha) = \xi\alpha$ for some n-th root of unity ξ. Details are left to you.

b) This is the harder part, and is the gateway to a whole slew of interesting phenomena. Rather than write out a formal proof, I'll present one way that one might discover a proof.

Let σ generate $G(E/F)$, and let ξ_n be a primitive n-th root of unity (such a thing exists thanks to hypothesis (i)). Now, σ is in particular an F-linear automorphism of the vector space E. Suppose σ has an eigenvector $\alpha \in E$, with eigenvalue ξ_n (which makes sense thanks to hypothesis (ii)). Then $\sigma(\alpha^n) = \alpha^n$ and hence $\alpha^n \in F$. Moreover the elements $1, \alpha, ..., \alpha^{n-1}$ are eigenvectors with distinct eigenvalues and so are linearly independent and hence a basis for E. Then we are done, since $F(\alpha) = E$.

How to find such an eigenvector? Let $\beta \in E$ and consider

$$\alpha = \sum_{i=0}^{n-1} \xi_n^{-i} \sigma^i(\beta).$$

An easy direct check shows $\sigma(\alpha) = \xi_n \alpha$, so if we can choose β so that $\alpha \neq 0$, we're done. But the sum above is zero for *all* β, then $\sum \xi_n^{-i} \sigma^i = 0$, contradicting the linear independence of automorphisms (Rotman Cor. 77). Done!

You might be wondering, however, how you would think of looking for the eigenvector in the first place, or of using the displayed equation. In fact there is a very natural way you might be lead to this approach, assuming your Galois theory brain is still on speaking terms with your representation theory brain. Consider for a moment a general finite Galois extension L/F, with group G. Then (ignoring the ring structure) G acts F-linearly on L, i.e. L is a representation of G over F. What representation is it? Here the Optimist Principle suggests the answer with such overwhelming moral force that it has to be true: Since $dim_F L = |G|$, what else could it be but the regular representation? And indeed this turns out to be correct, a result known as the Normal Basis Theorem. If there's time later, we'll prove it.

Meanwhile, even if the Normal Basis Theorem is only a conjecture, it suggests how to proceed with our cyclic extension. The assumptions on n imply that E is a completely reducible representation of our cyclic group G (Maschke's theorem), and that every irreducible representation of G is 1-dimensional. So as an FG-module, if our intuition is valid then E should split into the n 1-dimensional representations of G, and we get all our eigenvectors at once. In fact we even know how to carry out the splitting using our explicit formulas for idempotents in the group algebra; the displayed formula for α could have been written with a factor of $1/n$ in front of the sum, in which case it is exactly the idempotent associated to one of the irreducibles, applied to β.

Another approach to the proof is via "Hilbert's theorem 90", to be discussed in class. Among other things Theorem 90 has a claim to being the earliest appearance of homological algebra.

Theorem 4.1 is also the starting point of Kummer theory, a theory that at least gains a foothold for analyzing abelian extensions of fields. In short, Theorem 4.1 is well worth studying!

5 Radical and solvable extensions

I find it much more convenient to use the language of filtrations rather than that of "towers". We defined the concept of filtration in great generality long ago, for groups, modules, rings, topological spaces, etc.; in particular, a filtration of an extension E/F is just a chain of subextensions $F = K_0 \subset .... \subset K_n = E$ (we are assuming E/F is finite, so no interesting infinite filtrations are possible). I'll call the extensions K_i/K_{i-1} the *layers* of the filtration.

An extension E/F is a *radical extension* if it admits a filtration whose layers K_i/K_{i-1} are obtained adjoining an m_i-th root to a for some m_i and $a \in K_{i-1}$. An extension is *solvable by radicals* if it is contained in a radical extension. Finally, we need a definition of "solvable extension" E/F that doesn't require E/F to be Galois: We say that E/F is a solvable extension if $\tilde{E}/F$ has solvable Galois group. Note that this is equivalent to the existence of *some* finite Galois extension L/F with solvable Galois group and $E \subset L$.

Lemma 5.1 *The properties "radical" and "solvable" are preserved by splicing, base change, composites and split closures.*

Proof: We need only check splicing and base change. For the property "radical" these are very easy and left to the reader: Just splice the filtrations in the one case and "base change" the filtration in the other.

For the solvable case, first consider splicing (draw the diagram!). The Galois groups of $\tilde{E}/K$ and $\tilde{K}/F$ are solvable by assumption. Then $G(\tilde{E}/\tilde{K})$ is solvable since it is a subgroup of $G(\tilde{E}/K)$. It is also a normal subgroup of $G(\tilde{E}/F)$, with quotient $G(\tilde{K}/F)$, and since solvable groups are closed under extensions we are done.

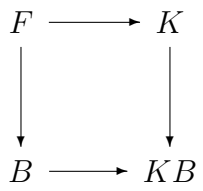
In the base change case, Let L/F be a solvable Galois extension containing K_1. Then LK_2/K_2 is Galois, and $G(LK_2/K_2)$ is isomorphic to a subgroup of $G(L/F)$ and so is solvable. Since $K_1K_2 \subset LK_2$, this shows that K_1K_2/K_2 is solvable.

Now, here is the main theorem of this section. We assume F has characteristic zero, and at the end comment on the characteristic p case. Note that now all splitting field extensions will be Galois extensions.

Theorem 5.2 *Suppose char $F = 0$. Then E/F is solvable by radicals if and only if it is solvable.*

Proof: Suppose E/F is solvable by radicals, i.e. lies in a radical extension K/F. Since radical extensions are preserved by split closure, we can assume K/F is Galois. Note that we then have $\tilde{E} \subset K$. Choose a radical filtration of K/F, and let m denote the product of all the m_i's that occur. Let $B = F(\mu_m)$, where μ_m is the group of m-th roots of unity.

We consider a diamond of extensions (please rotate!)



The base change KB/B is a radical Galois extension. In fact the base change of the radical filtration of K/F to KB/B has the same m_i's. (The layers of the base change filtration could be smaller than those of the original filtration, indeed could even be trivial, but this doesn't matter.) Then since B contains the m_i-th roots of unity for all i, we see that the layers are abelian Galois extensions. Applying the Galois correspondence yields a subnormal filtration of $G(KB/B)$ with abelian quotients, i.e. $G(KB/B)$ is solvable.

Since B/F is abelian, it follows that $G(KB/F)$ is solvable, so its quotient $G(K/F)$ is also solvable. Finally $G(\tilde{E}/F)$ is a quotient of $G(K/F)$, and so is solvable as desired.

For the converse we again consider a diamond as above, with the following changes of notation: Now $K = \tilde{E}$, so $G(K/F)$ is solvable by assumption, and we take $m = [K : F]$ (in the definition of B). By base change $G(KB/B)$ is solvable, so admits a subnormal filtration with cyclic quotients. Applying the Galois correspondence yields a filtration of KB/B whose layers are cyclic Galois extensions. Since the requisite roots of unity are present, Theorem 4.1 implies that each layer is obtained by adjoining a root of some element in the smaller field, so our extension is a radical extension. Since B/F is a radical extension, and radical extensions

are closed under splicing, KB/F is a radical extension. It contains $K = \tilde{E}$ and hence E, so E is solvable by radicals as desired.

Remark. Suppose F has characteristic p. Then there are two problems with extending the above theorem. First, the layers of a radical filtration need not be separable, so many of the Galois extensions entering into the proof will only be splitting fields in this case. This is only a technical difficulty, however, that can be dealt with. The more significant problem is that in characteristic p the theorem is just flat-out false as stated! There are cyclic (hence solvable) extensions of degree p that are not solvable by radicals, obtained by adjoining roots of polynomials of the form $x^p - x - a$ (see Rotman's problem 94). On the other hand, this doesn't mean we should give up and go home. It suggests that in characteristic p we need to modify the definition of a radical filtration, so that layers obtained from roots of $x^p - x - a$ are also allowed. With this modification, our theorem remains valid. See e.g. Lang for further discussion.