Chapter 5

Additional Topics

In this chapter we will look at some additional topics, related to field extensions and Galois Theory. Some of the results will be stated without proof, for the sake of time.

5.1 Transcendental Extensions

Back in Theorem 3.71 we showed that any algebraic extension can be broken into two pieces: a purely inseparable extension on top, and a separable extension at the bottom. In this section we take this one step further, to arbitrary extensions, by adding what is called a *purely transcendental* extension at the bottom. See Theorem 5.5.

Recall that for an extension F/K, a set of elements $A \subseteq F$ is *algebraically independent* over K if there is no polynomial equation relating them. In the special case $A = \{a\}$ of a singleton, A is algebraically independent over K iff a is transcendental over K. Recall from Corollary 3.5 that in this case $K(a)$ is isomorphic to $K(t)$, the field of rational functions in one variable t. For this reason, generic transcendental elements are often refered to as *variables*. The elements of an algebraically independent set are often called *independent variables*.

Definition 5.1 Let F/K be a field extension. A set $A \subseteq F$ is said to be

a *transcendence basis* for F over K is A maximal algebraically independent over K.

Proposition 5.1 *Given $S \subseteq T$ with S independent over K and F algebraic over $K(T)$, there is a transcendence basis B with $S \subseteq B \subseteq T$. In particular, any field extension F/K has a transcendence basis.*

Exercise 5.1.1

1. Prove that a directed union of algebraically independent sets over K is algebraically independent over K. In particular, the union of a chain of algebraically independent sets over K is algebraically independent over K.

2. Prove Proposition 5.1. Hint: use Zorn's lemma.

Algebraic independence for field extensions behaves somewhat like linear independence for vector spaces. For example, it is clear that a subset of an algebraically independent set is algebraically independent. The empty set is always algebraically independent. We will see below that algebraically independence also has an *exchange property*. (cf. Lemma 5.7) However, unlike the case of vector spaces, where a maximal independent set is also a generating set, in the case of field extensions, a maximal algebraically independent set is not necessarily a generating set.

Example 5.1.1 Let K be a field, and $F = K(t)$ the field of rational functions on t. The set $\{t\}$ is a transcendence basis for F over K. Let $L = F(t^{1/2}, t^{1/3})$. Even though both elements $t^{1/2}, t^{1/3}$ are transcendental over K, the set $\{t^{1/2}, t^{1/3}\}$ is not independent, since the polynomial $x_1^2 - x_2^3$ vanishes at them. In general, given any $r \in L$, since L/F is algebraic, there is $p(x) \in F[x]$ such that $p(r) = 0$. The coefficients of $p(x)$ are rational functions on t with coefficients in K, so, multiplying by the l.c.m. of the denominators of these coefficients, we can take $p(t, x) \in K[t, x]$ with $p(t, r) = 0$. Let $q(x_1, x_2) = p(x_1^2, x_2)$. Then we have $q(t^{1/2}, r) = p(t, r) = 0$, so the set $\{t^{1/2}, r\}$ is algebraically dependent. Thus we have, $\{t^{1/2}\}$ is a transcendence basis for L over K, even though $L \neq K(t^{1/2})$.

Definition 5.2 An extension F/K is said to be *purely transcendental* if there is a transcendence basis S of F over K, such that $F = K(S)$.

Examples 5.1.2

1. For the extension $F(t^{1/2}, t^{13})/F$ of Example 5.1.1, neither transcendence basis $\{t^{1/2}\}$ nor $\{t^{1/3}\}$, generates the whole field L. But if we take $u = \dfrac{t^{1/2}}{t^{1/3}}$ then $u^3 = t^{1/2}$ and $u^2 = t^{1/3}$, so $F(u) = L$ is puerly transcendental over K.

2. We will show that the extension $\mathbb{F}_4(t)/\mathbb{F}_2$ is not purely transcendental. This will require some work. See Example 5.1.3.

Lemma 5.2 *1. $S \subseteq F$ is algebraically independent over K iff every $\alpha \in S$ is transcendental over $K(S - \{\alpha\})$.*

2. If $S \subseteq F$ is algebraically independent over K and $\alpha \in F$ is transcendental over $K(S)$, then $S \cup \{\alpha\}$ is algebraically independent over K.

Proof. (1) ($\Rightarrow$) Assume some $\alpha \in S$ is algebraic over $E = K(S - \{\alpha\})$. Then there is a polynomial $f(x) \in E[x]$ such that $f(\alpha) = 0$. The coefficients of $f(x)$ are rational functions on $T = S - \{\alpha\}$ with coefficients on K. If we multiply $f(x)$ by a common multiple of the denominators of these rational functions, we get another polynomial $g(x) \in E[x]$ with $g(\alpha) = 0$, and the coefficients of $g(x)$ are in $K[T]$, i.e. $g(x) \in K[T, x]$. This shows that $T \cup \{\alpha\}$ is algebraically dependent.
($\Leftarrow$) Conversely, if S is algebraically dependent, there is a finite subset $\{\alpha_1, \ldots, \alpha_n\} \subseteq S$ and a non-zero polyomial $0 \neq f(X_1, \ldots, X_n)$ with $f(\alpha_1, \ldots, \alpha_n) = 0$. If we take this subset to be minimal, then α_n is algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$.
(2) Similar argument to (1,$\Leftarrow$). ■

Corollary 5.3 *Let $S \subseteq F$ be well-ordered. S is algebraically independent over K iff for every $\alpha \in S$, α is transcendental over $K(\{\beta \in S | \beta < \alpha\})$.*

Proof. ($\Rightarrow$) Follows from Lemma 5.2.1.
($\Leftarrow$) Repeat the argument in the proof of Lemma 5.2.1. ($\Leftarrow$) with $\alpha_1 < \cdots < \alpha_n$. ■

Proposition 5.4 *Let F/K be a field extension and $S \subseteq F$. TFAE:*

1. S is maximal algebraically independent over K.

2. *S is algebraically independent over K and F is algebraic over $K(S)$.*

3. *S is minimal such that F is algebraic over $K(S)$.*

Exercise 5.1.2 Prove Proposition 5.4. Hint: use Lemma 5.2.

Theorem 5.5 *For any extension F/K there is an intermediate field E such that F/E is algebraic and E/K is purely transcendental.*

Proof. Let S be a transcendence basis for F over K and $E = K(S)$. ■

The following theorem, which we will not prove, shows how far from unique the field E in Corollary 5.5 is.

Theorem 5.6 [Lüroth's Theorem, 1876] *Let t be transcendental over K. Let $K < F \leq K(t)$. There is $u \in F$ such that $F = K(u)$. Moreover, u is transcendental over K and t is algebraic over F, so $K(t)/F$ is algebraic and F/K is purely transcendental.*

Exercise 5.1.3 Let $u \in K[t]$ be a polynomial in t of degree n, then

$$\min_{K(u)}(t) = u(x) - u \quad \text{and} \quad [K(t) : K(u)] = n$$

We will show now that any two trascendence bases have the same cardinality. For that we will need the following *exchange property*, similar to the one for linear independence.

Lemma 5.7 [Exchange Property] *Let $S, T \subseteq F$ be each algebraically independent over K, with T a transcendence basis. For $\alpha \in S - T$ there is $\beta \in T - S$ such that $(S - \{\alpha\}) \cup \{\beta\}$ is algebraically independent over K.*

Proof. If we had every $\beta \in T - S$ algebraic over $K(S - \{\alpha\})$ then we would have $K(T)$ algebraic over $K(S - \{\alpha\})$. Since F is algebraic over $K(T)$, that makes α algebraic over $K(S - \{\alpha\})$, contradicting Lemma 5.2.1. Therefore, there is $\beta \in T - S$ transcendental over $K(S - \{\alpha\})$. By Lemma 5.2.2, $(S - \{\alpha\}) \cup \{\beta\}$ is algebraically independent. ■

Note 5.1 1. The *exchange property* is one of the defining axioms for what is called a *matroid*. A matroid consists of a set E, and a non-empty collection of subsets a set E, which is closed under taking subsets, and satisfies the exchange property. Examples of matroids include:

- the linearly independent subsets of a vector space,
- the linearly independent sets of columns of a given matrix,
- the algebraically independent sets in a field extension,
- the forests in a graph.

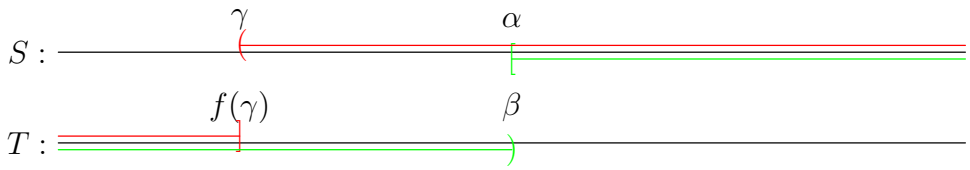
The concept of a basis is a matroid concept, and matroid theory is the natural context for the following theorem.

2. We should also note that there are many (equivalent) versions of the exchange property.

Theorem 5.8 *Any two transcendence bases of F/K have the same cardinality.*

Proof. Let S and T be transcendence bases for F/K. WLOG we may assume $S \cap T = \emptyset$, for if $U = S \cap T$, we may replace K with $K(U)$, S with $S - U$ and T with $T - U$. We want to show there is an injective map from S to T. Well-order S and define a function $f : S \to T$ recursively as follows. For $\alpha \in S$, we will consider the intervals:

$$\begin{array}{lcllcl} [-,\alpha) & = & \{\gamma \in S | \gamma < \alpha\} & [-,\alpha] & = & \{\gamma \in S | \gamma \leq \alpha\} \\ (\alpha,-) & = & \{\gamma \in S | \alpha < \gamma\} & [\alpha,-) & = & \{\gamma \in S | \alpha \leq \gamma\} \end{array}$$



Suppose f is already defined on $[-,\alpha)$ satisfying that for each $\gamma < \alpha$ the set $f\langle[-,\gamma]\rangle \cup (\gamma,-)$ is algebraically independent. We claim that the set $f\langle[-,\alpha)\rangle \cup [\alpha,-)$ is algebraically independent. If not, a dependence relation would involve finitely many elements of $f\langle[-,\alpha)\rangle$, and these elements would be in $f\langle[-,\gamma]\rangle$ for some $\gamma < \alpha$. Thus, the dependence relation is among elements of $f\langle[-,\gamma]\rangle \cup (\gamma,-)$, contradicting the assumption. Use now Lemma 5.7, with $\alpha \in f\langle[-,\alpha)\rangle \cup [\alpha,-) - T$, to choose $\beta \in T - (f\langle[-,\alpha)\rangle \cup [\alpha,-))$ such that $f\langle[-,\alpha)\rangle \cup [\alpha,-) - \{\alpha\} \cup \{\beta\}$ is algebraically independent, and define $f(\alpha) = \beta$. Then we have

$$f\langle[-,\alpha]\rangle \cup (\alpha,-) = f\langle[-,\alpha)\rangle \cup [\alpha,-) - \{\alpha\} \cup \{\beta\}$$

is algebraically independent, completing the recursive definition of f. It is clear that f is injective, since, by construction, $f(\alpha) \neq f(\gamma)$ for every $\gamma < \alpha$. Therefore, $|S| \leq |T|$. ■

Definition 5.3 The *transcendence degree* of F over K, denoted $tr.d._K(F)$ is the cardinality of a transcendence basis of F over K.

Exercise 5.1.4 Prove the following version of the exchange property: Let F/F be a field extension, $S, T \subseteq F$ be each algebraically independent over K with $|S| < |T|$, there is $\beta \in T - S$ such that $S \cup \{\beta\}$ is independent.

Example 5.1.3 As an application of Lüroth's theorem and Theorem 5.8, we can now see that $\mathbb{F}_4(t)/\mathbb{F}_2$ is not purely transcendental.

- Note first that $\mathbb{F}_4(t)/\mathbb{F}_2(t)$ is algebraic of degree 2; take $a \in \mathbb{F}_4 - \mathbb{F}_2$, and $\mathbb{F}_4(t) = \mathbb{F}_2(t)(a)$.
- It follows by Proposition 5.4, that $\{t\}$ is maximal algebraically independent in $\mathbb{F}_4(t)$ over $\mathbb{F}_2$. By Theorem 5.8, any transcendence basis is a singleton.
- Suppose now that $\mathbb{F}_4(t)/\mathbb{F}_2$ is purely transcendental, with transcendence basis S. Since $S = \{s\}$ is a singleton, and $\mathbb{F}_2 < \mathbb{F}_4 \leq \mathbb{F}_2(s)$, by Theorem 5.6 we would have $\mathbb{F}_4/\mathbb{F}_2$ purely transcendental, clearly a contradiction.

Proposition 5.9 *Given a tower $L/F/K$*

$$tr.d._K(L) = tr.d._F(L) + tr.d._K(F)$$

Exercise 5.1.5 Prove Proposition 5.9.