Lüroth's Theorem

Definition 1. *Let $u \in F(X) \setminus F$. Suppose $u = \frac{a(X)}{b(X)}$ where $a(X), b(X) \in F[X]$ and $gcd(a(X), b(X)) = 1$. Define degree of u to be*

$$deg(u) = max\{deg(a), deg(b)\}$$

Lemma 1. *Let $u \in F(X) \setminus F$. Then u is transcendental over F, X is algebraic over $F(u)$ and $[F(X) : F(u)] = deg(u)$*

Proof. Let $u = \frac{a(X)}{b(X)}$ with $\gcd(a(X), b(X)) = 1$. Now $a(T) - b(T)u$ is a polynomial in $F(u)[T]$ with X as a root. So $F(X)$ is algebraic over $F(u)$ and u is transcendental over F (otherwise X will be algebraic over F).
The polynomial $a(T) - b(T)Y \in F[T, Y]$ is irreducible because $a(T)$ and $b(T)$ are relatively prime. As u is transcendental over F, we have isomorphisms

$$F[T, Y] \simeq F[T, u], \quad T \leftrightarrow T, \quad Y \leftrightarrow u$$

so $a(T) - b(T)u$ is irreducible in $F[u, T]$, and hence is irreducible in $F(u)[T]$ by Gauss's lemma. It follows that

$$[F(X) : F(u)] = \deg(u).$$

□

Theorem 1 (Lüroth)**.** *Let $L = F(X)$ with X transcendental over F. Every subfield E of L properly containing F is of the form $E = F(u)$ for some u transcendental over F.*

Proof. Let $u \in F(X) \setminus F$. From the lemma

$$[F(X) : E] \leq [F(X) : F(u)] = \deg(u)$$

so X is algebraic over E. Let $[F(X) : E] = n$ and

$$f(T) = T^n + a_{n-1}T^{n-1} + ... + a_0, \quad a_i \in E$$

be the minimal polynomial of X over E. Since X is transcendental over F, there exists i such that $a_i \notin F$ (otherwise X will be algerbaic over F).
Let $d(X) \in F[X]$ be a polynomial of least degree such that $d(X)a_j(X) \in F[X]$ for all j, and let

$$f_1(X, T) = df(T) = dT^n + da_{n-1}T^{n-1} + ... + da_0 \in F[X, T] \tag{1}$$

Then f_1 is primitive as a polynomial in T (It is the primitive part of f). Let $a_n = 1$, so the coefficients of f_1 are $\{da_i\}_{i=0}^n$ when regarded as a polynomial in T. The degree m of f_1 in X is the largest degree of one of the polynomials $da_0(X), da_1(X), ..., da_n(X)$ say $m = \deg(da_i)$

Claim. *If $deg(da_i) = deg_X(f_1) = m$ then $a_i \notin F$. In particular $i \neq n$.*

Proof. Assume on the contrary $a_i \in F$. So $\deg(da_i(X)) = \deg(d(X)) \geq \deg(da_j(X))$ for $j \neq i$ which implies $\deg(d(X)X^n) > \deg(da_j(X)X^j)$ for all $j \neq n$. Because X is root of f_1, subsitutting $T = X$ in (1), we get

$$d(X)X^n + da_{n-1}(X)X^{n-1} + ... + da_0(X) = 0$$

$$\Rightarrow \deg(d(X)X^n) = \deg(da_{n-1}(X)X^{n-1} + ... + da_0(X)) < \deg(d(X)X^n)$$

Contradiction. □

Suppose $a_i(X) = \frac{b(X)}{c(X)}$ with b,c relatively prime polynomials in $F[X]$. From the claim $\deg(a_i(X)) \geq 1$ so $b(T) - c(T)a_i(X) \in E[T]$ is a non-constant polynomial. Now X is a root of $b(T) - c(T)a_i(X) \in E[T]$, so it is a factor of f, say

$$f(T)q(T) = b(T) - c(T)a_i(X), \quad q(T) \in E[T]$$

Multiplying the equation by $c(X)$, we get

$$c(X)f(T)q(T) = c(X)b(T) - c(T)b(X)$$

As f_1 is the primitive part of f, it divides $c(X)b(T) - c(T)b(X)$ in $F[X,T]$, so there exists a polynomial $h(X,T) \in F[X,T]$ such that

$$f_1(X,T)h(X,T) = c(X)b(T) - c(T)b(X) \tag{2}$$

In the above equation, the polynomial $c(X)b(T) - c(T)b(X)$ has degree at most $\max\{\deg(b), \deg(c)\}$ in X. Now $c(X)$ divides $d(X)$ so $\deg(c) \leq \deg(d)$ and thus $\deg(da_i) = \deg((\frac{d}{c})b) \geq \deg(b)$. It follows that

$$\deg(a_i) = \max\{\deg(b), \deg(c)\} \leq \max\{\deg(da_i), \deg(d)\} = \deg(da_i) = m \tag{3}$$

from our choice of index i so the polynomial $c(X)b(T) - c(T)b(X)$ in (2) has degree at most m. Also, f_1 has degree m in X therefore from equation (2) the polynomial $c(X)b(T) - c(T)b(X)$ has degree exactly m in X and because it is symmetric in X and T it has degree m in T also. It follows that $h(X,T)$ has degree 0 in X, so $h \in F[T]$. We claim that h is non-zero constant. Assume not, divide $h(T)$ from $b(T)$ and $c(T)$ to obtain

$$b(T) = \lambda_1(T)h(T) + r_1(T)$$

and

$$c(T) = \lambda_2(T)h(T) + r_2(T)$$

substituting this in (2) we obtain

$$f_1(X,T)h(T) = h(T)[c(X)\lambda_1(T) - b(X)\lambda_2(T)] + [c(X)r_1(T) - b(X)r_2(T)]$$

where $h(T)$ divides $[c(X)r_1(T) - b(X)r_2(T)]$ which has less degree in T than $h(T)$ so

$$[c(X)r_1(T) - b(X)r_2(T)] = 0 \Rightarrow c(X)r_1(T) = b(X)r_2(T)$$

but $\gcd(b(X), c(X)) = 1$ so $r_1(X)$ is a multiple of $b(X)$ and similarly $r_2(X)$ is a multiple of $c(X)$. Now as r_1, r_2 are remainders we have $\deg(r_1(X)) < \deg(b(X))$ and $\deg(r_2(X)) < \deg(c(X))$. Hence $r_1(X) = r_2(X) = 0$ implying $h(T)$ is common factor of $b(X)$ and $g = c(X)$ which contradicts the assumption that $b(X)$ and $c(X)$ are relatively prime.

So equation (2) becomes

$$f_1(X,T)h = c(X)b(T) - c(T)b(X)$$

so

$$\begin{aligned}[F(X) : E] = n = \deg_T(f_1) = \deg_T(c(X)b(T) - c(T)b(X)) \\ = m = \deg(da_i) \geq_{(3)} \deg(a_i) = [F(X) : F(a_i)] \geq [F(X) : E]\end{aligned}$$

Hence $E = F(a_i)$.

$\square$