

Let  $k$  be an arbitrary field and  $k(t)$  be a simple transcendental extension. We hope to understand intermediate extensions  $k \subset L \subset k(t)$ . To state Lüroth's theorem, we need a definition and a lemma:

**Lemma 1.** If  $f \in k(t)[x]$  is nonzero,  $f$  can be uniquely written

$$\frac{P(t, x)}{Q(t)}$$

in such a way that  $Q(t)$  and  $P(t, x)$  have no common factors in the UFD  $k[t, x]$ , and  $Q$  is monic.

*Proof.* First, write

$$f = \frac{p_0(t)}{q_0(t)} + \frac{p_1(t)}{q_1(t)}x + \dots + \frac{p_n(t)}{q_n(t)}x^n.$$

Then, we can note that

$$f = \frac{\sum_{i=0}^n q_0(t) \cdot \dots \cdot q_i(t) \cdot \dots \cdot q_n(t) p_i(t) x^i}{q_0(t) \cdot \dots \cdot q_n(t)}.$$

Now we have expressed  $f$  as a fraction of polynomials in  $k[t, x]$ . Since  $k[t, x]$  is a UFD, we can write the fraction in a reduced form. The reduced form is unique if we further multiply both numerator and denominator by a constant term such that the denominator is monic.  $\square$

**Definition 1.** Let  $u \in k(t)[x]$ . By the previous lemma, there exists unique  $P, Q$ , where  $Q$  is monic, such that

$$u = \frac{P(t, x)}{Q(t)}.$$

We define the **height of  $u$**  to be the number

$$\max(\deg_t(P), \deg_t(Q)).$$

We first go through some lemmas before stating Lüroth's theorem.

**Lemma 2.** If  $f \in k(t)[x]$  ( $f = \frac{P(t, x)}{Q(t)}$ ) is monic in  $x$ ,

$$\text{ht}(f) = \deg_t(P(t, x)).$$

Furthermore, we have that  $P(t, x)$  is not divisible by any non-unit of  $k[t]$ .

*Proof.* First, write

$$f(x) = \frac{p_n(t)x^n + \dots + p_0(t)}{Q(t)}.$$

Because  $f$  is monic,  $p_n(t) = Q(t)$ , implying  $\deg_t(P) \geq \deg_t(Q)$ . A restatement of the second conclusion of the theorem is that  $\gcd(p_0, p_1, \dots, p_n) = 1$ . Since the expression above is assumed to be a reduced fraction, no factor of  $Q$  also divides all  $p_i$  simultaneously. This means

$$\gcd(Q, p_0, p_1, \dots, p_n) = 1.$$

But  $Q = p_n$  implies

$$\gcd(p_0, p_1, \dots, p_n) = 1.$$

$\square$

**Corollary 1.** If  $f, g \in k(t)[x] - \{0\}$ , are monic in  $x$ ,

$$\text{ht}(f \cdot g) = \text{ht}(f) + \text{ht}(g).$$

*Proof.* We have  $f \cdot g$  is monic in  $x$ . If  $f = \frac{P}{Q}$  and  $g = \frac{P'}{Q'}$ ,

$$f \cdot g = \frac{P \cdot P'}{Q \cdot Q'}.$$

This fraction is in a reduced form and  $Q \cdot Q'$  is monic. Hence

$$\text{ht}(f \cdot g) = \deg_t(P \cdot P') = \deg_t(P) + \deg_t(P') = \text{ht}(f) + \text{ht}(g)$$

by the lemma. □

**Lemma 3.** Let  $u \in k(t) \setminus k$ . There exists  $u' \in k(t) \setminus k$  such that  $k(u') = k(u)$  where  $u' = \frac{P'}{Q'}$ ,  $\deg_t(P) > \deg_t(Q)$ , and  $P', Q'$  are monic.

*Proof.* First, we know  $u = \frac{P}{Q}$  by Lemma . If  $\deg_t(Q) < \deg_t(P)$ , we can just multiply  $u$  by a constant to achieve the desired  $u'$ . Otherwise, we can select  $\beta \in k$  such that  $\deg(P + \beta Q) < \deg(Q)$ . We can write

$$u' = \alpha * \frac{Q}{P + \beta Q}$$

where  $\alpha$  is chosen so that the resulting fraction has monic numerator and denominator. Note that  $Q$  and  $P + \beta Q$  do not have common factors. In either case, note  $u \in k(u')$  and  $u' \in k(u)$ , so  $k(u) = k(u')$ . □

**Lemma 4.** Given  $u = \frac{P(t)}{Q(t)} \in k(t) - k$ , verify that  $t$  is a root of  $P(x) - uQ(x) \in k(u)[x]$ . Show further that if  $\deg_t(P) > \deg_t(Q)$ , and  $P$  is monic, then the above polynomial is monic.

*Proof.* The first assertion is just

$$P(t) - \frac{P(t)}{Q(t)}Q(t) = 0.$$

The second claim is just because the leading coefficient of  $P(x) - uQ(x)$  is equal to that of  $P(x)$  if  $\deg_t(P) > \deg_t(Q)$ . □

We would like to prove the following theorem:

**Theorem 1.** (Lüroth's Theorem) Let  $k$  be an arbitrary field. If  $k(t)$  is a simple transcendental extension of  $k$ , and

$$k \subset L \subset k(t).$$

is an arbitrary intermediate field extension  $L \neq k$ , then  $L$  is also a simple transcendental extension over  $k$ , generated by an element  $u \in k(t)$  of minimal possible height. We further have  $[L : k] = \text{ht}(u)$ .

The proof requires some steps. Given  $u$  an element of minimal height in  $L - k$ , we write

$$u = \frac{P(t)}{Q(t)}$$

using Lemma , and denote the height of  $u$  by  $n \in \mathbb{Z}$ . By Lemma , we can assume that  $\deg(P) > \deg(Q)$  and  $P$  is monic.

**Lemma 5.** For any  $f \in L[x]$ ,  $\text{ht}(f)$  is either 0 or is at least  $n$ .  $P(x) - uQ(x)$  is either irreducible in  $L[x]$  or is divisible by a non-unit element of  $k[x]$ .

*Proof.* We also show that  $P(x) - u \cdot Q(x)$  has height  $n$ . By Lemma , we can construct  $f' = \frac{P'}{Q'}$  such that both numerator and denominator are monic with

$$\deg_t(P') > \deg_t(Q').$$

By construction of  $u$ ,  $\text{ht}(f') \geq \text{ht}(u) = n$  or  $\text{ht}(f') = 0$ . The conclusion is given by  $\text{ht}(f) = \text{ht}(f')$ . We calculate

$$\text{ht} \left( P(x) - \frac{P(t)}{Q(t)} Q(x) \right) = \text{ht} \left( \frac{P(x)Q(t) - P(t)Q(x)}{Q(t)} \right).$$

Note that  $Q(t)$  does not share a factor with  $P(x)Q(t) - P(t)Q(x)$ , for then it would share a factor with  $P(t)Q(x)$ . Because  $k[t, x]$  is a UFD, this would mean  $Q(t)$  shares a factor with  $P(t)$ . In particular, the expression in the height above is the fraction expression used in the definition of height. The height is thus

$$\max(\deg_t(P(x)Q(t) - P(t)Q(x)), \deg_t(Q(t))) = \max(\deg_t(P(t)), \deg_t(Q(t)))$$

because  $\deg(P) > \deg(Q)$ . The second conclusion is from the fact that if  $P(x) - uQ(x) = s(t, x)w(t, x)$  for  $s, w \in L[x]$ , we can assume  $s, w$  are monic in  $x$  since  $P(x) - uQ(x)$  is. Corollary 1 says that  $\text{ht}(s) + \text{ht}(w) = \text{ht}(P(x) - uQ(x)) = n$ . Hence one of  $\text{ht}(s), \text{ht}(w)$  is 0 and one of them is  $n$ .  $\square$

**Lemma 6.** If  $P(x) - uQ(x)$  is divisible in  $L[x]$  by an element in  $k[x]$ , then this element must divide both  $P(x)$  and  $Q(x)$ . Deduce that this element must be a unit.

*Proof.* The second claim immediately follows from the first because we assume  $\frac{P}{Q}$  is a reduced fraction. To prove the first claim, if  $P - uQ$  is divisible by an element  $s(x) \in k[x]$  in  $L[x]$ , we have there exists  $w(x, t) \in L[x]$  such that

$$s(x)w(x, t) = P(x) - uQ(x).$$

In  $L$ , we can extend  $\{1, u\}$  to a basis for  $L$  as a  $k$ -vector space using Zorn's lemma. Say

$$L = k \oplus k \cdot u \oplus W.$$

for complementary  $k$ -vector subspace  $W \subset L$ . Denote the  $L$  coefficients for  $P, Q, w, s$  by  $P_i, Q_i, w_i, s_i$  respectively (in the first two cases they are coefficients in  $k$ ) and

$$w_i(t) = a_i + b_i u + c_i(t)$$

for  $w_i(t) \in L$ ,  $a_i, b_i \in k$ , and  $c_i(t) \in W$ . Then for all  $i$ ,  $s(x) \cdot w(x, t) = P(x) - uQ(x)$  gives

$$\sum_{j+k=i} s_j(a_k + b_k u + c_k(t)) = P_i - uQ_i.$$

By linear independence,

$$s(x) \cdot (a_0 + a_1 x + \dots + a_{\deg_x(w)} x^{\deg_x(w)}) = P$$

and

$$s(x) \cdot (b_0 + b_1 x + \dots + b_{\deg_x(w)} x^{\deg_x(w)}) = Q.$$

$\square$

Finally, we can prove Lüroth's theorem as follows.  $P(x) - uQ(x)$  is an irreducible polynomial with  $t$  as a root. This implies that  $P(x) - uQ(x)$  is a minimal polynomial of  $t$  over  $L$  and  $k(u)$ . In particular,

$$[L : k] = [k(u) : k] = \deg(P(x)).$$

Hence, we have  $[L : k(u)] = 1$  and  $L = k(u)$ .