

We are going to prove something called Lüroth's Theorem. For a little biography of Lüroth, see

<http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Luroth.html>

The theorem comes from the study of rational parametrizations of curves.

An affine variety  $V$  is a curve if any proper algebraic subset  $W \subsetneq V$  is finite.

Suppose  $V_1, V_2$  are affine curves and  $V_1 \xrightarrow{\mathbb{F}} V_2$  is a polynomial map.

We get a homomorphism

$$F^* = \Gamma(V_2) \rightarrow \Gamma(V_1).$$

Since  $\Gamma(V_2)/\ker(F^*) \cong \text{Im}(F^*) \subseteq \Gamma(V_1)$

and  $\Gamma(V_1)$  is a domain,  $\ker(F^*)$  is a prime ideal of  $\Gamma(V_2)$ .

By the definition of curve, though, the only prime ideals of  $\Gamma(V_2)$  are  $\{0\}$  and the maximal ideals (exercise!). So, either:

(1)  $\ker(F^*) = \{0\}$ , i.e.  $F^*$  is injective,

or

(2)  $\ker(F^*)$  is a maximal ideal.

Suppose we are in case (2), and let

$\mathfrak{m} = \ker(F^*)$ . Since maximal ideals

of  $\Gamma(V_2)$  correspond to points of  $V_2$ ,

there is a point  $p \in V_2$  such that

$$\mathfrak{m} = \mathcal{I}(\{p\}).$$

Lemma In this case,  $F(V_1) = \{p\}$ .

Proof. Suppose  $a \in V_1$  and  $F(a) = q$ . If  $f \in \Gamma(V_2)$  then  $F^*(f)(a) = f(F(a)) = f(q)$ .

Now  $f \in \mathfrak{m} \Rightarrow F^*(f) = 0 \Rightarrow f(q) = 0$ ,

so  $q \in V(\mathfrak{m}) = V(\mathcal{I}(\{p\})) = \{p\}$ .  $\square$

So, there are two possibilities: either  $\Gamma(V_1)$  consists of a single point, or

$$\Gamma(V_2) \cong \text{Im}(F^*) \subseteq \Gamma(V_1).$$

In the latter case, we get an injective homomorphism of fields,

$$k(V_2) = \text{Frac}(\Gamma(V_2)) \hookrightarrow \text{Frac}(\Gamma(V_1)) = k(V_1).$$

Lüroth's Theorem Suppose  $K \subseteq k(t)$  is a subfield with  $k \subsetneq K$ . Then  $K \cong k(u)$ . More precisely, there is an element  $u \in k(t)$  such that  $K = k(u)$ .

In particular, if there is a polynomial map  $\mathbb{A}_k^1 \rightarrow V_2$  whose image consists of more than one point, then

$$k(V_2) \cong k(t).$$

The proof of Lüroth's theorem takes a few pages.

## Some Algebraic Preliminaries

Def let  $K \subseteq E$  be fields. An element  $e \in E$  is algebraic over  $K$  if there is a nonzero polynomial

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in K[x] \text{ such that}$$

$$f(e) = a_0 + a_1e + \dots + a_n e^n = 0.$$

[ $e$  satisfies a polynomial equation over  $K$ .]

An extension of fields  $K \subseteq E$  is finite if there exist  $e_1, \dots, e_n \in E$  such that

$$E = K \cdot e_1 + \dots + K \cdot e_n,$$

i.e.  $E$  is a finite-dimensional

$K$ -vector space. If  $E$  is finite over  $K$ ,

the degree of the extension is

$$[E : K] = \dim_K(E).$$

Suppose  $K \subseteq E$  is a field extension and  $e \in E$  is algebraic over  $K$ . Let

$$J_e = \{ f \in K[x] \mid f(e) = 0 \}.$$

Lemma  $J_e$  is a nonzero ideal in  $K[x]$ .

Pf. Just check.  $\square$

Def A minimal polynomial  $p_e(x)$  of  $e$  in  $K$  is a generator of  $J_e$ , i.e.  $J_e = (p_e)$ .

So,  $p_e(e) = 0$  and if  $f(e) = 0$  then  $p_e(x)$  divides  $f(x)$ .

Lemma A minimal polynomial of  $e$  in  $K$  is irreducible.

Proof. Suppose  $p_e(x)$  is a minimal polynomial of  $e$ .

If  $p_e(x) = f(x)g(x)$  then  $0 = p_e(e) = f(e)g(e)$

$\Rightarrow$  either  $f(e) = 0$  or  $g(e) = 0$ . If  $f(e) = 0$ , then  $p_e \mid f$  and  $f \mid p_e \Rightarrow f$  equals  $p_e$  times

a unit. It follows (check!) that  $g$  must be a unit in  $K[x]$  (i.e. a constant).  $\square$

Note that, if  $e \in E$ , then, defining  
$$ev_e: K[x] \rightarrow E \text{ by}$$
$$ev_e(f) = f(e),$$

$\mathcal{J}_e = \ker(ev_e)$ . So

$$K[x]/\mathcal{J}_e \cong \text{im}(ev_e).$$

By the lemma,  $\mathcal{J}_e$  is a prime ideal,  
hence maximal since  $K[x]$  is a PID.

Corollary  $\text{Im}(ev_e)$  is a subfield of  $E$   
that contains both  $K$  and  $e$ .

Def We write  $K(e) = \text{Im}(ev_e)$ .

This is the smallest subfield of  $E$   
that contains both  $K$  and  $e$ .

To reiterate, all of this discussion applies if  $e$   
is algebraic over  $K$ . If  $e$  is not algebraic  
over  $K$ , we say  $e$  is transcendental over  $K$ .

Examples  $\sqrt{2}$  is algebraic over  $\mathbb{Q}$ .

$\pi$  is transcendental over  $\mathbb{Q}$ .

If  $e \in E$  is transcendental over  $K$ , the

homomorphism  $ev_e: K[x] \rightarrow E$

$$ev_e(f) = f(e)$$

is injective. Since  $E$  is a field, we

thus get a homomorphism (injective!)

$$K(x) \xrightarrow{ev_e} E$$

$$ev_e\left(\frac{f(x)}{g(x)}\right) = \frac{f(e)}{g(e)}.$$

We also write  $K(e) = \text{Im}(ev_e)$  in this case. Again,  $K(e)$  is the smallest subfield of  $E$  that contains  $K$  and  $e$ ; but this time  $K(e) \cong K(x)$ .

We will need the following shortly:

General Lemma let  $K$  be a field and

$p(x) \in K[x]$  irreducible of degree  $n$ . Then

$$\dim_K K[x]/(p(x)) = n.$$

Proof of General Lemma.

$$p(x) = c_0 + \dots + c_{n-1}x^{n-1} + c_n x^n; \quad c_n \neq 0.$$

Note that  $1, x, \dots, x^{n-1}$  are linearly independent in  $K[x]/(p(x))$  iff

$$\lambda_0 \cdot 1 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} = 0, \text{ it means}$$

$\lambda_0 + \lambda_1 x + \dots + \lambda_{n-1} x^{n-1} \in (p(x))$ , which is clearly impossible unless  $\lambda_0 = \lambda_1 = \dots = \lambda_{n-1} = 0$ .

I claim that  $1, x, \dots, x^{n-1}$  span  $K[x]/(p(x))$ .

Indeed, it suffices to prove that

$x^{n+k}$  is in the span of  $1, x, \dots, x^{n+k-1}$

for all  $k \geq 0$ . But  $\frac{1}{c_n} x^k p(x) = 0$  in  $K[x]/(p(x))$ ,

$$\text{so } x^{n+k} = -\frac{1}{c_n} (c_0 x^k + \dots + c_{n-1} x^{n+k-1})$$

in  $K[x]/(p(x))$ , which gives what we need.  $\square$

Lemma Suppose  $u \in k(t)$  and  $u \notin k$ . Then  $u$  is transcendental over  $k$ .

Proof. Write  $u = \frac{f(t)}{g(t)}$  with  $f$  and  $g$  relatively prime (i.e. a reduced fraction).

Suppose  $a_0 + a_1 u + \dots + a_n u^n = 0$  with

$a_0, \dots, a_n \in k$ . Then, multiplying by  $g^n$ , we get

$$a_0 g^n + a_1 g^{n-1} f + \dots + a_{n-1} f g^{n-1} = -a_n f^n$$

Now  $g$  divides LHS but  $g$  is relatively prime to the RHS unless  $a_n = 0$ . We conclude that  $a_n = 0$ . So  $u$  cannot satisfy a polynomial equation of degree  $n$  for any  $n \geq 1$ .  $\square$

Lemma Suppose  $u \in k(t)$ ,  $u \notin k$ , and write

$u = \frac{f(t)}{g(t)}$  a reduced fraction. Let

$m = \max \{ \deg(f), \deg(g) \}$ . Then

(1)  $t$  is algebraic over  $k(u)$ .

(2)  $[k(t) : k(u)] \leq m$ .

Proof. Let

$$f(t) = a_0 + a_1 t + \dots + a_n t^n,$$

$$g(t) = b_0 + b_1 t + \dots + b_m t^m.$$

Then

$$(b_0 + b_1 t + \dots + b_m t^m) u = a_0 + \dots + a_n t^n, \text{ or}$$

$$(b_0 u - a_0) + (b_1 u - a_1) t + \dots + (b_m u - a_m) t^m = 0.$$

This proves (1).

Next, the degree of the minimal polynomial  $P_t$

of  $t$  over  $k(u)$  is  $\leq m$ . We thus get

$$k(t) = \Sigma_m (\text{ev}_t : k(u)[x] \rightarrow k(t)) \cong k(u)[x]/(P_t).$$

So (2) follows from the general lemma.  $\square$

Corollary of the lemma If  $u = \frac{at+b}{ct+d}$  and

(i) either  $a \neq 0$  or  $c \neq 0$

(ii)  $(a,b)$  is not a scalar multiple of  $(c,d)$ ,

then  $k(u) = k(t)$ .

Proof. By the previous lemma, the conclusion will follow if  $u \notin k$ . Conditions (i) and (ii) are exactly what's needed to rule that out.  $\square$

Another Corollary of the lemma If  $k \subsetneq K \subsetneq k(t)$ ,  $K$  a field, then  $t$  is algebraic over  $K$ .

Pf. Choose any  $u \in K \setminus k$ . Then  $t$  is alg. over  $k(u)$  and  $k(u) \subseteq K$ .  $\square$ .

We're almost ready for Lüroth's Theorem.

We need one more lemma, but for that we need to recall Gauss's Lemma.

Def Let  $D$  be a unique factorization domain; and  $0 \neq f = \sum_{i=0}^n a_i x^i \in D[x]$ .

The content  $C(f)$  of  $f$  is a GCD of  $a_0, \dots, a_n$ .

Recall let  $a_0, \dots, a_n \in D$ . A GCD of  $a_0, \dots, a_n$  is an element  $d \in D$  such that

(i)  $d \mid a_i$  for  $i=0, 1, \dots, n$ .

(ii) If  $c \mid a_i$  for  $i=0, 1, \dots, n$  then  $c \mid d$ .

Note If  $u \in D$  is a unit then  $ud$  is also a GCD of  $a_0, \dots, a_n$ .

Gauss lemma If  $D$  is a UFD and  $f, g \in D[x]$ , then " $C(fg) \sim C(f)C(g)$ " (one side equals the other side times a unit).

Def  $f \in D[x]$  is primitive if  $C(f) \sim 1$ .

Corollary let  $D$  be a UFD,  $F = \text{Frac}(D)$ .

Suppose  $f, g \in D[x]$ . Suppose  $f$  is primitive and  $f$  divides  $g$  in  $F[x]$ . Then  $f$  divides  $g$  in  $D[x]$ .

Example

$D = \mathbb{Z}$ ,  $F = \mathbb{Q}$ . Then  $f = 2x + 2$  does not divide  $g = x + 1$  in  $\mathbb{Z}[x]$  but it does in  $\mathbb{Q}[x]$  — it's because  $f$  is not primitive; the 2 causes a problem in  $\mathbb{Z}[x]$  but it becomes a unit in  $\mathbb{Q}[x]$ .

Proof of Corollary. Write  $g = f \cdot h$ , where  $h \in F[x]$ .

let  $d = \text{LCM}(\text{denominators of coeff. of } h)$ , so

$dh \in D[x]$  but  $\text{GCD}(d, dh) = 1$ .

We also have  $dg = f \cdot dh$  in  $D[x]$ . Then

$$d \cdot C(g) = C(dg) \stackrel{\text{Gauss}}{=} C(f)C(dh) = C(dh),$$

$\uparrow$   
 $f$  is primitive

so  $d$  divides  $C(dh)$ , which implies

$d \mid \text{GCD}(d, dh)$ . Thus  $d$  is  
a unit in  $D$ , and

$$dh \in D[x] \Rightarrow h \in D[x]. \quad \square.$$

We will apply the corollary for

$$D[x] = k[t][x],$$

$$F[x] = k(t)[x],$$

$k$  a field.

Lüroth's Theorem  $k \subsetneq K \subseteq k(t)$ ,  $k$  a field. Then  $K = k(u)$  for some  $u \in k(t)$ .

Proof of Lüroth's Thm.

Let

$f(x) = x^n + \frac{c_1}{d} x^{n-1} + \dots + \frac{c_n}{d} \in k[x]$  be the min. poly. of  $t$  over  $K$  (recall  $t$  is algebraic over  $K$ !), so  $\frac{c_i}{d} \in K$ ,

$c_i(t), d(t) \in k[t]$ ,  $n = [k(t) : K]$ ,

and we have chosen  $d$  minimal:

$$\text{GCD}(c_0, \dots, c_{n-1}, d) = 1.$$

Note Not all  $c_i/d$  can be in  $k$ . ( $t$  is not alg. over  $k$ ).

Suppose  $u = \frac{c_j}{d} \notin k$  and write  $u = \frac{g}{h}$  with  $g, d \in k[t]$  and  $\text{GCD}(g, h) = 1$ .

Note Then  $h \mid d$ , say  $d = h \cdot l$  with  
 $l = l(t) \in k[t]$ .

Let  $m = \max \{ \deg(g), \deg(h) \}$ .

We have:

$$n = [k(t) : K] \leq [k(t) : k(u)] \leq m$$

$\uparrow$  a lemma

and:

If  $n = m$  then  $K = k(u)$ .

Note This follows from easy lemma: if  
 $E \subseteq K \subseteq F$  are fields and each is  
a finite-dimensional vector space over  
the last, then

$$[F : E] = [F : K][K : E].$$

We will prove that  $n=m$ , which, by the boxed statement, finishes the proof.

To start, observe that  $t$  is a root of

$$g(x) - u(t)h(x) \in K[x].$$

So, by def of min poly,  $\exists r(x) \in K[x]$  with

$$g(x) - u(t)h(x) = r(x)f(x).$$

Clearing denoms gives

$$(*) \quad g(x)h(t) - g(t)h(x) = h(t)r(x)f(x).$$

OTOH, set

$$\mathcal{F}(x,t) \stackrel{d.f.}{=} d(t)f(x) = h(t)l(t)f(x).$$

Note

$$\deg_x(\mathcal{F}) = n, \text{ still.}$$

By construction,

$$\text{GCD}(\text{coeff of } \mathcal{F}) = \text{GCD}(c_0, \dots, c_{n-1}) = 1.$$

By (\*)  $\mathcal{F}$  divides  $g(x)h(t) - g(t)h(x)$   
in  $k(t)[x]$ .

But  $\mathcal{F}$  is primitive (this is exactly the GCD statement), so  $\mathcal{F}$  divides it also in  $k[t][x]$ . We get the crucial eq.

$$(*) \quad Q(x,t) \mathcal{F}(x,t) = g(x)h(t) - g(t)h(x) = h(t) \cdot (x) \cdot f(x) \\ \text{in } k[t][x].$$

This will allow us to conclude that  $m = n$ .

Step 1  $\deg_t(\text{center}) = \deg_x(\text{center}) = m.$

This gives

$$m = \deg_t(Q \cdot \mathcal{F}) \geq \deg_t(\mathcal{F}) = \deg_t(d \cdot f)$$

$$\geq \max \{ \deg(d), \deg(f) \}$$

(first one is clear, second one since  $\deg_t(d \cdot f)$  is  $\geq \deg_t$  of any of its coeff, and  $\frac{c_j}{d} = \frac{g}{h}$ ).

$$\geq \max \{ \deg(h), \deg(g) \} = m.$$

(since  $h$  divides  $d$ )

$$\Rightarrow m = \deg_t(Q \cdot \mathcal{F}) = \deg_t(\mathcal{F})$$

$$\Rightarrow \mathbb{Q}(x, t) = \mathbb{Q}(x) \in k[x].$$

Step 2 By Step 1, the GCD of coeff.

of  $Q$  is a unit in  $k[t]$ , i.e.  $Q$  is primitive in  $k[t][x]$ . So is  $\mathcal{F}$ , we saw. By Gauss lemma, this implies

$$Q \cdot \mathcal{F} \text{ primitive} \stackrel{(t)}{\implies} g(x)h(t) - g(t)h(x) \text{ primitive "in } x \text{"}$$

symmetric in  $t$  and  $x$

$$\implies g(x)h(t) - g(t)h(x) \text{ primitive in } t$$

$$\implies Q(x) \mathcal{F}(x/t) \text{ primitive in } t$$

$$\implies Q(x) \in k.$$

Step 3 From Step 1,  $n = \deg_t(\mathcal{F})$ .

By def of  $\mathcal{F}$ ,  $n = \deg_x(\mathcal{F})$ .

By Step 2 and (t), both of these

equal  $\deg_t(\text{content of } (t))$ . Done!  $\square$