Lüroth's theorem

Thm (Lüroth). Let F be a field and x transcendental$/F$. Let $F(x)/E/F$. Then $\exists u \in F(x)$ s.t. $E = F(u)$.

We will have to consider $F(x)[t]$ in our analysis.
The key tool is Gauss' lemma.

Setup R a UFD, $K = \mathrm{Frac}(R)$.
We seek to compare factorization in $R[t]$ and $K[t]$.

Def. Let $f \in R[t]$. Write $f = \sum_{i=0}^{n} a_i t^i$. Then $c(f) = \gcd(a_0, \ldots, a_n)$ is the content of f. We say f is primitive if $c(f) \in R^\times$, i.e. its coefficients are coprime.

e.g. $2t+1 \in \mathbb{Z}[t]$ is primitive
$xt + x \in F[x][t]$ has content x.

Roughly, factoring in $R[t]$ is the same as factoring in $K[t]$ except for irreducible factors of the content.
$2t+2 \in \mathbb{Z}[t]$ reducible
$2t+2 \in \mathbb{Q}[t]$ irreducible

Facts
- $R[t]$ is a UFD
- Let $f \in K[t] - \{0\}$. Then $f = \alpha f_1$ with $\alpha \in F^\times$, $f_1 \in R[t]$ primitive. This factorization is unique up to units in R.

- "Gauss' lemma" $c(fg) \approx c(f)c(g)$

Pf. clear denominators and factor out a gcd.

Lemma. $t^n - x \in F(x)[t]$ is irreducible

Pf. This polynomial is in $F[x][t]$ and is primitive, so it's irreducible in $F(x)[t] \iff$ it's irreducible in $F[x][t]$.

Approach 1. $t^n - x \in F[x][t]$ is irreducible by Eisenstein's criterion on the prime x. $\square$

Approach 2. $F[x][t] = F[x,t] = \underbrace{F[t][x]}$
$-x + t^n$ is linear, hence irreducible. $\square$

Finally, recall some results from the homework.

7. $F < E \subseteq F(x) \implies x$ algebraic $/E$

36. Let $f, g \in F[t]$ coprime, $u = f/g \in F(t) - F$.

a) $[F(t) : F(u)] = \max(\deg(f), \deg(g))$

b) All elements of $G(F(t)/F)$ are of the form
$$t \longmapsto \frac{at+b}{ct+d} \quad \text{for} \quad ad - bc \neq 0$$

Rmk. 36.b) defines a surjective homomorphism
$$GL_2(F) \longrightarrow G(F(t)/F)$$
one checks that its kernel is $Z(GL_2(F)) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \middle| \lambda \in F^\times \right\}$,

so $G(F(t)/F) \cong PGL_2(F)$.

Now, we prove Lüroth's theorem.

Take $F < E \subseteq F(x)$. By HW7, $F(x)/E$ is algebraic,

So there's a minimal polynomial $m_E(x) \in E[t]$

Note that: $m_E(x)$ is <u>not</u> a polynomial in x! To avoid confusion, let $\tilde{f} = m_E(x)$.

We may write $f(t) = a(x)\tilde{f}(t)$ for $a \in F[x]$, $f \in F[x][t]$ primitive.

Write $f = \sum_{i=0}^{n} a_i(x) t^n$, $a_i(x) \in F[x]$,

As $\tilde{f}(t)$ is monic, $a_n(x) = a(x)$ in $F[x]$,

we write $n = \deg_t(f)$

$= \deg_t(m_E(x))$ (only t makes sense, really)

$= [F(x) : E]$

As x is transcendental $/F$ and $\tilde{f}(x) = 0$, $\tilde{f}(t) \notin F[t]$,

Thus, as $f(t) = a(x)\tilde{f}(t)$, $\exists i$ s.t. $u = a_i(x)/a(x) \notin F$,

Write $u = g(x)/h(x)$ for $g, h \in F[x]$ coprime,

By HW36.a, $[F(x) : F(u)] = \max(\deg(g), \deg(h))$, which we

denote by r. Hence,

$$n = [F(x) : E] \leq [F(x) : F(u)] = r$$

So $n \leq r$. We seek $r \leq n$.

Now, let $d(x,t) = g(x)h(t) - h(x)g(t) \in F[x,t]$.

Notice that $d = \det \begin{pmatrix} g(x) & h(x) \\ g(t) & h(t) \end{pmatrix}$. Hence, as g and h are

coprime in $F[x,t]$, $d(x,t) \neq 0$.

Consider $u(x)h(t) - g(t) = \frac{1}{h(x)} d \in E[t]$. This polynomial

vanishes when $t = x$, as $d(x,x) = 0$.

Thus, $\tilde{f} = m_E(x) \mid h(x)^{-1} d$ in $E[t]$

Thus, $f \mid h(x)^{-1} d$ in $F(x)[t]$.

$f(t)$ primitive in $F[x][t]$, and $d \in F[x][t]$, so we must have $f \mid d$ in $F[x][t]$, by Gauss' lemma.

Write $d = f\alpha$, $\alpha \in F[x,t]$.

$$\begin{aligned} \deg_x(d) &= \deg_x(g(x)h(t) - h(x)g(t)) \\ &\leq \max(\deg_x g(x), \deg_x h(x)) \\ &= r \end{aligned}$$

$$\begin{aligned} \deg_x(f) &= \deg_x\left(\sum_{j=0}^{n} a_j(x)t^j\right) \\ &= \max(\deg_x a_i(x) \mid 0 \leq i \leq n) \\ &\geq \max(\deg_x a_i(x), \deg_x(a_n(x))) \end{aligned}$$

Recall $u = g(x)/h(x) = a_i(x)/a_n(x)$, so indeed

$$\begin{aligned} \deg_x(f) &\geq \max(\deg_x g(x), \deg_x h(x)) \\ &= r \end{aligned}$$

On the other hand, $f(x) \mid d(x)$ in $F[x,t]$, so

$$r \leq \deg_x f(x) \leq \deg_x d(x) \leq r$$

And we attain equality,

Thus, $\deg_x(\alpha) = 0$, so $\alpha \in F[t]$,

Hence, $\alpha \in F[x][t]$ is primitive $/F[x]$.

Gauss' lemma then says $d = f\alpha$ is primitive in $F[x][t]$,

Furthermore, $d(x,t) = -d(t,x)$, so d is also primitive in $F[t][x]$,

$\alpha \in F[t]$, $\alpha \mid d$ in $F[t][x]$ so as d is primitive, $\alpha \in F[t]^\times = F^\times$.

Thus,

$$\begin{aligned}
[F(x):E] &= n \\
&= \deg_t(f) \\
&= \deg_t(d) \\
&= \deg_x(d) \\
&= \deg_x(f) \\
&= r \\
&= [F(x):F(u)]
\end{aligned}$$

So $E = F(u)$. $\square$

Rmk. - $F(x) \cong F(u)$ via $x \mapsto u$.

More formally, consider the map

$$\begin{aligned} F[x] &\longrightarrow F(u) \\ x &\longmapsto u \end{aligned}, \text{ i.e. } f(x) \mapsto f(u)$$

This is injective as u is transcendental$/F$. Hence, all non zero elements become units in $F(u)$, so by the universal property of localization, we get a map $F(x) \longrightarrow F(u)$. This is an iso$/F$.

- This is an algebraic analogue of the fact that the if X is a connected compact Riemann surface with a holomorphic map $\mathbb{CP}^1 \xrightarrow{f} X$ which is nonconstant, then $X \cong \mathbb{CP}^1$.

Indeed, $M(X) \xhookrightarrow{f^*} M(\mathbb{CP}^1) \cong \mathbb{C}(z)$

$\varphi \longmapsto \varphi \circ f$

field of meromorphic functions

yields $M(\mathbb{CP}^1)/M(X)/\mathbb{C}$, so $M(X) = \mathbb{C}(\varphi)$ for some $\varphi \in \mathbb{C}(z)$.

this field $\longleftrightarrow$ connected compact Riemann surface dictionary is exceptionally strong (and is an equivalence of categories

$\{K/\mathbb{C} \mid K \text{ f.g. and tr deg}(K/\mathbb{C}) = 1\}^{op} \simeq \{\text{connected compact Riemann surfaces}\}$)

For instance, one may recall that $\mathrm{Aut}(\mathbb{CP}^1)$ is precisely the set of Möbius transformations

$$z \longmapsto \frac{az+b}{cz+d}$$

for $a, b, c, d \in \mathbb{C}$ s.t. $ad - bc \neq 0$, and indeed, $\mathrm{Aut}(\mathbb{CP}^1) \cong PGL_2(\mathbb{C})$,

so $\mathrm{Aut}(\mathbb{CP}^1) \cong GL(\mathbb{CP}^1)/\mathbb{C}$!