Friday: review (I'll post references to other topics)

Today: Transcendental & infinite ext'ns

Def: $S \subseteq E$ is alg. dep. over $F \subseteq E$ if $\exists$ poly.

$f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ and $a_1, \dots, a_n \in S$ s.t. $f(a_1, \dots, a_n) = 0$.

Otherwise, S is alg. indep. over F.

A maximal alg. indep. set is called a transcendendance basis for E/F

Thm: a) Any ext'n E/F has a transcendance basis

b) If S_1, S_2 are transcendance bases for E/F, then $|S_1| = |S_2|$ (called the transcendance degree)

Examples: a) If E/F alg., then trans. basis $= \phi$

trans. degree $= 0$

b) If $E = F(\overset{\text{trans.}/F}{t})$,

$\{t\}$ and $\{t^2\}$ are both trans. bases of E/F

But $F(t) \neq F(t^2)$

Def: E/F is purely transcendental if it has a trans. basis S w/ $E = F(S)$

Ex: $\mathbb{Q}(t, \sqrt{t^3 - t}) / \mathbb{Q}$ not purely trans. (Ex 14.9.6)

Thm: Let t be trans. $/F$.

1) If $F \subseteq K \subseteq F(t)$, $F \neq K$, then K is purely trans. $/F$

2) Let $P(t), Q(t) \in F[t]$, not both constant, w/ $\gcd(P, Q) = 1$.

Then,

$$[F(t) : F(P/Q)] = \max(\deg P, \deg Q)$$

3) $F(P/Q) = F(t) \iff P, Q$ are coprime deg ≤ 1 polys., not both constant

i.e. $F(r) = F(t) \iff r = \underbrace{\frac{at+b}{ct+d}}_{\text{fractional linear transformation}}, \; ab - bc \neq 0$

Therefore, $\mathrm{Aut}(F(t)/F) = \left\{ t \mapsto \frac{at+b}{ct+d} \right\}$

Surj. homom.

$$GL_2(F) \longrightarrow \mathrm{Aut}(F(t)/F)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left(t \mapsto \frac{at+b}{ct+d} \right)$$

kernel is $\left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right\}$, so

$$\mathrm{Aut}(F(t)/F) \cong PGL_2(F)$$

See D&F p. 647-8 for case where $F = \mathbb{F}_2$

Def: E/F is Galois if E/F alg., sep., and E is a splitting field $/F$ for some set of polys. in $F[x]$.

In this case, $\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F)$.

Note: not necessarily a bijection btwn. int. fields and subgroups of $\mathrm{Gal}(E/F)$.

Ex: Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots) \subseteq \mathbb{R}$ alg. ✓

char $E = 0 \Rightarrow$ separable ✓

E: splitting field for $\{x^2-2, x^2-3, \dots\}$ ✓

So $E/\mathbb{Q}$ is Galois

If $\sigma \in G := \mathrm{Gal}(E/\mathbb{Q})$,

$$\sigma(\sqrt{2}) = \pm\sqrt{2}$$
$$\sigma(\sqrt{3}) = \pm\sqrt{3}$$
$$\vdots$$

So $G \cong \underset{\langle\sigma_2\rangle}{\mathbb{Z}_2} \times \underset{\langle\sigma_3\rangle}{\mathbb{Z}_2} \times \underset{\langle\sigma_5\rangle}{\mathbb{Z}_2} \times \cdots$

Uncountably many subgps. of index 2

But only countably many int. fields w/ deg. $2/\mathbb{Q}$: $\mathbb{Q}(\sqrt{p})$

Too many subgps.

Idea: Krull topology

If $F \subseteq E_1 \subseteq E_2$ and E_1/F, E_2/F Galois,

then $\exists$ restriction homom.

$$\mathrm{Gal}(E_2/F) \longrightarrow \mathrm{Gal}(E_1/F)$$
$$\sigma \longmapsto \sigma|_{E_1}$$

Turns out $\mathrm{Gal}(E/F)$ is the <u>projective limit</u> or <u>inverse limit</u> of all $\mathrm{Gal}(K/F)$, K/F finite. That is, there is a restriction homom. $\mathrm{Gal}(E/F) \xrightarrow{\varphi} \mathrm{Gal}(K/F)$, and every elt. of $\mathrm{Gal}(K/F)$ maps nontrivially to some $\mathrm{Gal}(K/F)$, K/F finite.

$\ker \varphi = \mathrm{Gal}(E/K)$ and cosets are the subsets of $\mathrm{Gal}(E/F)$ which map to a single element of $\mathrm{Gal}(K/F)$

Let a Krull subgp. be any subgp. of $\mathrm{Gal}(E/F)$ made up of a union of these cosets (for various K).

Thm: $\exists$ bij.
$$\left\{ \begin{array}{c} \text{int fields} \\ F \subseteq E' \subseteq E \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Krull subgps.} \\ H \leq \mathrm{Gal}(E/F) \end{array} \right\}$$

and the lattices are dual. Also,

$$\begin{array}{l} H \leq \mathrm{Gal}(E/F) \\ H : \text{Krull} \\ H : \text{normal} \end{array} \iff \mathrm{Fix}\, H \text{ is Galois} / F$$

Ex: $F = \mathbb{F}_p$. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}_n$

Saw in §14.3 that $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$, so

$$\underbrace{\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)} \xrightarrow[\text{restr.}]{} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}_n$$

$$\hat{\mathbb{Z}} := \{ v = (v_1 \bmod 1, v_2 \bmod 2, v_3 \bmod 3, \dots) \text{ s.t. } m \mid n \Rightarrow v_m \equiv v_n \bmod m \}$$

$\mathbb{Z} \subsetneq \hat{\mathbb{Z}}$ by $n = (n \bmod 1, n \bmod 2, n \bmod 3, \dots)$