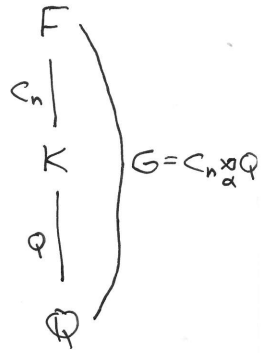
LECTURE 3

We have seen that not every C_2-extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$ can be embedded in a C_8-extension (or even C_4, by Witt #1), or in a Q_8-extension (d must be sum of 3 squares by Witt #2)

but for $C_4 \times C_2$ and D_4 the embedding problem always has a solution:

Thm (Saltman) Let $G = A \rtimes \mathbb{Q}$ with A abelian. A regular $\mathbb{Q}$-extension $K/\mathbb{Q}(t_1, \ldots, t_n)$ can be embedded in a regular G-extension of $\mathbb{Q}(t_1, \ldots, t_n)$.

I know an explicit version when $A = C_n$ is cyclic:



Thm Q finite group, $n \geq 2$.

$\alpha : Q \longrightarrow \mathrm{Aut}\, C_n$ homomorphism

$K/\mathbb{Q}$ Galois with Galois group Q, $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$

As before, identify

$$\mathrm{Gal}(K(\zeta_n)/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma_j : \zeta_n \mapsto \zeta_n^j \longleftrightarrow j$$

For $g \in K(\zeta_n)$, define

$$f_g(x) = \prod_{\ell \in \mathbb{Z}/n\mathbb{Z}} \left(x - \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \zeta_n^{\ell k} \prod_{\substack{j \in (\mathbb{Z}/n\mathbb{Z})^\times \\ q \in Q}} A_{q, \alpha(q)^{-1} j k} \right) \quad ; \quad A_{q,j} := \sqrt[n]{\sigma_j(q(g))}.$$

Then $f_g(x) \in \mathbb{Q}[x]$. For most choices of g it is irreducible, and $F = \mathbb{Q}(\text{roots of } g)$ has $\mathrm{Gal}(F/\mathbb{Q}) = C_n \rtimes_\alpha Q$.

Rmk Implemented as Extension(Q-family, G, A) $\rightsquigarrow$ G-family.

§8 Examples

Ex $S_3 \twoheadrightarrow C_2$ split extension; kernel $A = C_3$.
(G, Q)

← when $|Q|$ and $|A|$ are coprime, by Schur-Zassenhaus every extension is split

Thm $\Rightarrow$ every quad. ext. $\mathbb{Q}(\sqrt{a})$ is contained in a S_3-field, for example

$$x^3 - 3(a^2+a+1)x + 2(a-1)(a^2+a+1)$$

← see homepage for code; regular

Ex $D_n = C_n \rtimes C_2$ $\Rightarrow$ D_n can be realised over $\mathbb{Q}(a)$, regularly.

Again, these families can be quite unwieldy for large n; see Problem 6.

We have constructed regular families for cyclic groups, and abelian groups are also easy (e.g. x^2-a regular family for C_2 over $\mathbb{Q}(a)$ $\Rightarrow$ $(x^2-a)(x^2-b)$ regular family for C_2^2 over $\mathbb{Q}(a,b)$, and similarly for all direct products).

Looking at small non-abelian groups, we see that $C_n \rtimes Q$ construction covers many of them:

$S_3 = C_3 \rtimes C_2$

$D_4 = C_4 \rtimes C_2$

* Q_8 ⟵ not a semidirect product

$D_5 = C_5 \rtimes C_2$

A_4 ⟵ covered by Hilbert's A_n-result, and Saltman's $A \rtimes Q$ Thm. $[A = C_2^2,\ Q = C_3]$

$D_6 = C_2 \times S_3 = C_6 \rtimes C_2$

$Dic_3 = C_4 \rtimes C_3$ or see Q3

$D_7 = C_7 \rtimes C_2$

...

In fact, we can construct Q_8 over $\mathbb{Q}(a)$ as well because Q_8 is a quotient of $C_4 \rtimes C_4$ of order 16 (SmallGroup(16,4)) to which theorem applies:

```
G := SmallGroup(16,4);                                   G = C4 ⋊ C4
S := [D`subgroup: D in NormalSubgroups(G)];
assert exists(A){A: A in S | #A eq 4 and IsCyclic(A) and IsCyclic(quo<G|A>)};
                                                         A = C4 ◁ G; Q = G/A = C4
QF := Family(4,1);
F := Extension(QF, G, A);                                apply thm. to G ↠ Q
G := Group(F);
S := [D`subgroup : D in NormalSubgroups(G)];
assert exists(N){N: N in S | #N eq 2 and GroupName(quo<G|N>) eq "Q8"};
f := Subfield(F,N);                                      Q8 - quotient
Family(f);
```

Exc $\mathcal{I}_{G/\mathbb{Q}(t)}$ is true for $G = Q_8, Q_{16}, Q_{32}, \ldots$ ← generalised quaternion groups; see Question Q8.

Rmk These constructions avoid the study of obstructions to the embedding problem!

§9 Semiabelian groups.

What have we done so far? Apart from S_n, A_n, we have regular realisations $/\mathbb{Q}(t)$ of

- Cyclic groups
- Split extensions $A \rtimes Q$ when A is abelian, and Q has a regular realisation $/\mathbb{Q}(t)$.

It is also not hard to realise direct products and wreath products:

- $\mathcal{I}_{G/\mathbb{Q}(t)}, \mathcal{I}_{H/\mathbb{Q}(t)} \Rightarrow \mathcal{I}_{G\times H/\mathbb{Q}(t)}$
- $\mathcal{I}_{G/\mathbb{Q}(t)}, \mathcal{I}_{H/\mathbb{Q}(t)} \Rightarrow \mathcal{I}_{G\wr H/\mathbb{Q}(t)}$

← this uses regularity, and the corresponding claims for $\mathcal{I}_{G/\mathbb{Q}}$ are less clear. For example, it is not known that $SL_2(\mathbb{F}_{16}) \times SL_2(\mathbb{F}_{16})$ is a Galois group over $\mathbb{Q}$, because only one example of a $SL_2(\mathbb{F}_{16})$ extension is known (Bosman 2020).

These constructions generate a class of groups, called semiabelian:

Thm (Matzat, Dentzer, Stoll) The following conditions on a finite group G are equivalent:

- G can be obtained in finitely many steps from C_1 by taking split extensions of abelian groups and taking quotients
  $[G_0 = C_1,\ G_1 = A_0 \rtimes G_0,\ G_2 = G_1/N_1,\ G_3 = A_2 \rtimes G_2,\ G_4 = G_3/N_3, \ldots, G_k = G]$
- G is generated by abelian subgps $A_1, \ldots, A_n$ with $A_i \subseteq N_G A_j$ for $i \leq j$.
- G is a quotient of $C_m \wr C_m \wr \cdots \wr C_m$ (k times) for some $m, k \geq 1$.

A group satisfying these conditions is called semiabelian.

By Saltman's Theorem, $\mathcal{I}_{G/\mathbb{Q}(t)}$ is true for G semiabelian.

Properties

- semiabelian groups $\subsetneq$ soluble groups.
- semiabelian groups are closed under quotients, direct products, wreath products,
- If G is generated by A and U with $A \trianglelefteq G$ abelian, $U \lneq G$ semiabelian then G is semiabelian, and conversely.
- If G is nilpotent of class 2 ($G' < Z(G)$) then G is semiabelian (Thompson)
- If G is soluble with all Sylows abelian then G is semiabelian (Thompson)
- If G has order p^n, $n \leq 4$ or 2^5 then G is semiabelian (Dentzer).

Of the 319 groups of order < 64 only 5 are not semiabelian:

$SL_2(\mathbb{F}_3)$, $C_2 \cdot S_4$, $GL_2(\mathbb{F}_3)$, $C_2 \times SL_2(\mathbb{F}_3)$, $SL_2(\mathbb{F}_3) : C_2$, A_5

$= 2O = csu_2(\mathbb{F}_3) = SL_2(\mathbb{F}_3) \cdot C_2$

all related to $SL_2(\mathbb{F}_3)$ — not soluble

§10 $SL_2(\mathbb{F}_3)$

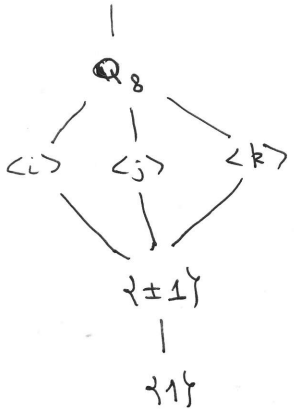
— Quite a lot of attention has been devoted to the group $2A_4 = Sl_2(3)$. Despite this, no explicit polynomial giving a geometric extension of $\mathbb{Q}(t)$ with Galois group $2A_4$ seems to be known.

G. N. Smith, Some polynomials over $\mathbb{Q}(t)$ and their Galois groups, 1999.

$SL_2(\mathbb{F}_3)$ is a very interesting group in many contexts (e.g. largest automorphism group of an elliptic curve). Its group structure is:

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ $\quad i^2 = j^2 = k^2 = -1$, $ij = k$, $ki = j$, $jk = i$ ← has an obvious automorphism action $\varphi : C_3 \to \mathrm{Aut} Q_8$

$SL_2(\mathbb{F}_3) = Q_8 \rtimes_\varphi C_3$



↷ permuted by φ

$= Z(SL_2(\mathbb{F}_3))$

Galois correspondence