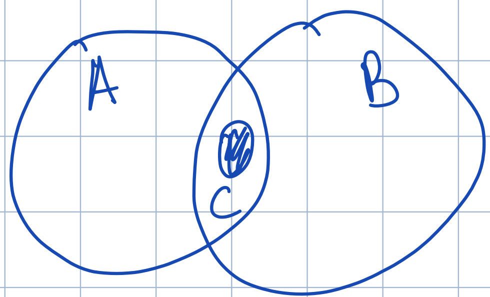
Composita & further comments on the main thm

Lecture 22

Let A, B be two sets. Then the intersection $A \cap B$ can be defined using just the operation $\subseteq$: indeed, $A \cap B \subseteq A, B$ and $A \cap B$ is the maximal set having this property: $\forall C$ s.t. $C \subseteq A, B \Rightarrow C \subseteq A \cap B$.



We use this idea to make some further comments on the Galois correspondence.

Now let $H_1, H_2 \leq G$ and we have L^{H_1}, L^{H_2}. Then $H_1 \cap H_2 \leq G$ is the maximal subgroup in H_1, H_2, hence by the Galois correspondence $L^{H_1 \cap H_2}$ is the minimal subfield of L s.t. $L^{H_1 \cap H_2}$ contains L^{H_1} and L^{H_2}.

Df. Let K_1, K_2 be some subfields of L. The compositum of K_1 and K_2 in L (or the composite field), denoted by K_1K_2, is the smallest subfield of L containing both K_1 & K_2.

Ex. Let $K - K(A) := E$, $K - K(B) := F$. (some subsets of L)
Then EF is $K(A \cup B)$. Indeed, EF must contain $K, A, B \Rightarrow K(A \cup B)$ and, obviously

$K(A), K(B) \subseteq K(A \cup B)$. E.g., $\mathbb{Q}(\alpha)\cdot\mathbb{Q}(\beta)$
$= \mathbb{Q}(\alpha,\beta)$

L. Let $K, E, F \subseteq L$. Suppose that
1) If $[E:K], [F:K] < \infty$, then $[EF:K] < \infty$
2) If $E:K, F:K$ are normal, then $E \cap F : K$ is normal
3) If $[E:K], [F:K] < \infty$ and $E:K$ is normal, then $EF:F$ is normal.
4) If $E:K, F:K$ are finite & normal, then $EF:K$ & $E \cap F : K$ are normal.
5) If $E:K, F:K$ are normal & finite, then $EF : E \cap F$ is a normal ext.

Pf. 1) We have $E = K(A)$, $|A| < \infty \Rightarrow$ $EF = F(A) \Rightarrow [EF:F] \leq \prod_{a \in A} [F(a):F] < \infty$ (use the tower law) Thus by the tower law again $[EF:K] = [EF:F][F:K] < \infty$.

2) Take $\forall \alpha \in E \cap F$ and since $E:K$ is algebraic over $K \Rightarrow \alpha$ is algebraic over $K \Rightarrow$ $E \cap F : K$ is algebraic. Now let $f \in K[t] \setminus K$ s.t. $f(\alpha) = 0$ & f is irr. over $K \Rightarrow f$ splits over E & $F \Rightarrow f$ splits over $E \cap F$.

3) Since $E:K$ is normal & finite $\Rightarrow \exists$ $g \in K[t] \setminus K$ s.t. E is the splitting field

of g. Let $\alpha_1, \dots, \alpha_d \in E$ be the roots of g, $E = K(\alpha_1, \dots, \alpha_d) \Rightarrow EF = F(\alpha_1, \dots, \alpha_d)$ (as in the 1st part) $\Rightarrow EF:F$ is a splitting field extension for g and hence $EF:F$ is normal.

4) As in the 3rd part: $E:K$ is a splitting field of $g \in K[t] \setminus K$ & $F:K$ is a splitting field for $h \in K[t] \setminus K$, $E = K(A)$, $F = K(B)$, where A, B are roots of $g, h \Rightarrow EF = K(A \cup B)$ $\Rightarrow EF:K$ is a splitting field of $gh \Rightarrow$ normal

5) We have $K - \underbrace{E \cap F - EF}_{\text{normal by part 4}} \Longrightarrow$

$E \cap F - EF$ is normal. $\blacksquare$

Exm. $\mathbb{Q} - \mathbb{Q}(i)$ is normal and
$\mathbb{Q} - \mathbb{Q}(\sqrt[3]{2}) =: \alpha$ is not normal. By the lemma above (part 3)
$\mathbb{Q}(i)\mathbb{Q}(\alpha) = \mathbb{Q}(i, \alpha) : \mathbb{Q}(\alpha)$ is normal (indeed, it is the splitting field for t^2+1)
but $\mathbb{Q}(i)\mathbb{Q}(\alpha) : \mathbb{Q}$ is not normal ($t^3 - 2$ does not split over $\mathbb{Q}(i) \cdot \mathbb{Q}(\alpha)$, we need to „adjoint $\sqrt{3}$")

Let us return to the Galois correspondence. We have $H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \mapsto L^{H_1} L^{H_2}$.

Similarly, if $P, Q \subset L$ are subfields, then
$P \cap Q \longmapsto \langle G_P \cup G_H \rangle$ (i.e. $L^{\langle G_P \cup G_H \rangle}$)

Is it true that $\langle G_P \cup G_H \rangle = G_P G_H$? (*)
If so, then $G_P G_H = \langle G_P \cup G_H \rangle = G_H G_P \Rightarrow$
either $G_P \trianglelefteq G$ or $G_Q \trianglelefteq G$ (and clearly, this is enough for (*))

Exm. Let $\gcd(m,n)=1$. Then one has
$\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$.

Indeed, $\mathrm{Gal}_{\mathbb{Q}}\, \mathbb{Q}(\varepsilon_{nm}) = \mathbb{Z}_{nm}^* = \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ (1)
$|G| = \varphi(nm) = \varphi(n)\varphi(m)$

$$\begin{tikzcd}
 & \mathbb{Z}_{mn}^* \arrow[dl, dash, "\varphi(n)"'] \arrow[dr, dash, "\varphi(m)"] & \\
\mathbb{Z}_m^* \arrow[dr, dash, "\varphi(m)"'] & & \mathbb{Z}_n^* \arrow[dl, dash, "\varphi(n)"] \\
 & \mathrm{Id} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, dash, "\varphi(n)"'] \arrow[dr, dash, "\varphi(m)"] & \\
\mathbb{Q}(\varepsilon_n) \arrow[dr, dash, "\varphi(m)"'] & & \mathbb{Q}(\varepsilon_m) \arrow[dl, dash, "\varphi(n)"] \\
 & \mathbb{Q}(\varepsilon_{nm}) &
\end{tikzcd}$$

Clearly, $\mathbb{Z}_m^* \cap \mathbb{Z}_n^* = \{\mathrm{Id}\} \Rightarrow \mathbb{Q}(\varepsilon_n) \cap \mathbb{Q}(\varepsilon_m)$
corresponds $L^{\mathbb{Z}_{mn}^*} = \mathbb{Q}$ (we use (1)).

Exm From algebra we know that

$$G = N \times H \iff \begin{cases} NH = G \\ N \cap H = \{\mathrm{Id}\} \\ N, H \trianglelefteq G \end{cases} \qquad \left(\Rightarrow \langle N, H\rangle = NH = HN\right)$$

Using the Galois correspondence, we

see that this is equivalent to

$$\begin{cases} K - L^N, \; K - L^H \text{ are normal} \\ L^N L^H = L^{\{Id\}} = L \\ L^N \cap L^H = L^G = K. \end{cases}$$

In terms of fields: $\begin{cases} P:K, \; Q:K \text{ are normal} \\ PQ = L \\ P \cap Q = K \end{cases}$

$\Leftrightarrow G = G_P \times G_Q$. This is a criterium of the fact that $Gal_K(f_1 f_2) \cong Gal_K f_1 \times Gal_K f_2$

(recall the example, Lecture 18:
$f_1 = x^2 + x + 1$, $f_2 = x^2 + 3$, $f = f_1 f_2$ but
$Gal_{\mathbb{Q}}(f) \not\cong Gal_{\mathbb{Q}}(f_1) \times Gal_{\mathbb{Q}}(f_2)$. Indeed,
$P = Q = L = \mathbb{Q}(i\sqrt{3})$ and hence $P \cap Q \neq \mathbb{Q}$)

How did solvable (soluble) groups come about?

For simplicity, assume that $\operatorname{char} K = 0$, $\sqrt{1} \subset K$ and $K - L$ is a radical Galois extension. In other words, we have the following extension (we have that $L:K$ is Galois)

$$K = K_0 - K_1 - K_2 - \ldots - K_m = L, \quad K_j = K_{j-1}(r_j)$$
$$r_j^{n_j} \in K_{j-1}$$

$$\mathrm{Gal}_K L = G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{\mathrm{Id}\}$$

By assumption $\sqrt[\infty]{1} \subset K \Rightarrow K_j : K_{j-1}$ is a normal extension (we adjoint a root r of $t^n - r$ and hence all roots of this polynomial) Thus $G_j \trianglelefteq G_{j-1}$ and we obtain

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots \triangleright G_m = \{\mathrm{Id}\}$$

This is a subnormal series. We can consider

normal ⊕ $K_{j-1} - K_j$ is normal

$$\begin{array}{ccccc} K_{j-1} & - & K_j & - & L \\ G_{j-1} & & G_j & & \{\mathrm{Id}\} \end{array}$$

By definition

$$\Rightarrow G_j = \mathrm{Gal}_{K_j} L \text{ and } G_{j-1}/G_j \cong \mathrm{Gal}_{K_{j-1}} K_j$$

(we have used the main theorem several times) But $\mathrm{Gal}_{K_{j-1}} K_j = \mathrm{Gal}_{K_{j-1}}(t^{n_j} - r_j)$ and this is a subgroup in $\mathbb{Z}_{n_j}$ (hence this is a cyclic group). Thus, we have arrived to the definition:

Df. A group G is said to be soluble if $\exists$ a finite series of subgroups

$$\{e\} = G_n \leq G_{n-1} \leq \ldots \leq G_1 \leq G_0 = G \quad \text{s.t.}$$

(1) $G_j \trianglelefteq G_{j-1}$, $\forall\ 1 \leq j \leq n$ and

(2) G_{j-1}/G_j is cyclic, for $1 \leq j \leq n$.

We will consider soluble groups next time.

Ex. $E:K$, $F:K$ are finite, $K, E, F \subseteq L$. Then:

1) If $E:K$ is separable, then $EF:F$ is separable

2) If $E:K$, $F:K$ are both separable, then $EF:K$ and $E \cap F:K$ are separable.