defined.

2. Study solvable groups and establish in particular that this property is inherited by subgroups and quotients.

In order to motivate 2. we will now achieve 1. under an additional technical assumption, later to be removed.

Lemma III.9

Let $k = K_0 \subset K_1 \subset \dots K_t$ be a tower of extensions where

1.) K_t/k is normal.

2.) K_i/K_{i-1} is pure of type p_i

$1 \leq i \leq t$, p_i a prime.

3.) k contains all p_i'th roots of 1.

Then there is a sequence of subgroups

$$G = \mathrm{Gal}(K_t/k) = G_0 \supset G_1 \supset \cdots \supset G_t = (e)$$

with $\quad G_i \triangleleft G_{i-1} \qquad 1 \leq i \leq t$

$\qquad G_{i-1}/G_i$ is either trivial or

$$\cong \mathbb{Z}/p_i\mathbb{Z} \quad .$$

<u>Proof</u>: Define $\quad G_i = \mathrm{Gal}(K_t/K_i)$

in particular $\quad G_0 = \mathrm{Gal}(K_t/k) = G$

and since $\quad K_{i-1} \subset K_i \quad$, we have

$$G_i = \mathrm{Gal}(K_t/K_i) \subset G_{i-1} = \mathrm{Gal}(K_t/K_{i-1})$$

Now $\quad K_i = K_{i-1}(u_i)$ with $u_i^{p_i} \in K_{i-1}$.

Let $\quad f_i(x) = X^{p_i} - c_i \,,\; c_i = u_i^{p_i}$.

Then $f_i \in K_{i-1}[x]$;

~~irreducible~~ since k and hence K_{i-1}

contains all p_i'th roots of 1, K_i is a splitting field of f_i. If f_i is not irreducible, then (lemma III.5) c_i is a p_i'th power in K_{i-1} and hence K_{i-1} contains all the roots of f_i, implying $K_i = K_{i-1}$, that is $u_i \in K_{i-1}$. But this contradicts the assumption that K_i is a pure extension of prime type.

Hence f_i is irreducible and lemma III.5 implies that $Gal(K_i | K_{i-1})$ is either trivial or $\cong \mathbb{Z}/_{p_i \mathbb{Z}}$.

Finally observe that we have

$$K_{i-1} \subset K_i \subset K_t$$

and that both K_i and K_t are normal extensions of K_{i-1}. This implies that

$$G_i = \mathrm{Gal}(K_t / K_i) \triangleleft G_{i-1} = \mathrm{Gal}(K_t / K_{i-1})$$

and $\quad G_{i-1} / G_i \cong (e)$ or $\mathbb{Z}/p_i\mathbb{Z}$. $\square$

A finite group with the property of lemma III.9 belongs to the class of solvable groups. This notion applies to all groups, finite or not, and therefore has to be reformulated differently.

Given a group G, recall that the subset

$$G^{(1)} = [G,G] := \{ [x_1, y_1] \cdots [x_{r}, y_r] : (x_1, y_1, \ldots, x_r, y_r) \in G^{2r},\ r \geq 1 \}$$

where $[x,y] := xyx^{-1}y^{-1}$

is a subgroup of G. Indeed

(1) $[x,x] = e$

(2) $[x,y]^{-1} = [y,x]$.

It is not only a normal subgroup but it is even characteristic.

<u>Def. III.10</u> a subgroup $H < G$ is characteristic if $\varphi(H) = H$ $\forall \varphi \in \operatorname{Aut} G$.

Recall that every $g \in G$ gives rise to an automorphism $\operatorname{int}(g) \in \operatorname{Aut} G$ defined by $\operatorname{int}(g)(h) := g h g^{-1}$. In this way we obtain a homomorphism

$$\operatorname{int} : G \longrightarrow \operatorname{Aut} G$$

whose image $\operatorname{Int}(G)$ is the subgroup of all inner automorphism. From this viewpoint a subgroup $H < G$ is normal iff $\operatorname{int}(g)(H) = H$ $\forall g \in G$. In particular a characteristic subgroup is normal.

Here is a crucial property of characteristic subgroups:

Lemma III.11 Let $L < H < G$ be subgroups. Assume

(1) $H \triangleleft G$

(2) L is a characteristic subgroup of H.

Then $L \triangleleft G$.

Proof: For every $g \in G$ we have, $\mathrm{int}(g)(H) = H$. Thus $\mathrm{int}(g)|_H \in \mathrm{Aut}\, H$, not necessarily inner, and since L is characteristic in H, $\mathrm{int}(g)(L) = L$. $\boxed{\Sigma}$

Now define inductively

$$G^{(1)} = [G, G],$$
$$G^{(2)} = [G^{(1)}, G^{(1)}], \ldots$$

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}], \quad n \geq 2.$$

Since for every $n \geq 2$, $G^{(n)}$ is characteristic in $G^{(n-1)}$, it follows that

$$G^{(n)} \triangleleft G \quad \forall n \geq 1.$$

<u>Definition III. 12</u> The sequence $G \supset G^{(1)} \supset G^{(2)} \supset \ldots$ is the derived series of G.

<u>Definition III. 13</u> The quotient

$G_{ab} := G/G^{(1)}$ is called the abelianization of G.

<u>Lemma III. 13</u>

(1) the group $G_{ab} = G/G^{(1)}$ is abelian.

For every homomorphism $\varphi : G \to A$ into an abelian group A, there is a unique homomorphism $\bar{\varphi} : G_{ab} \to A$ such that the diagramm

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & A \\ G_{ab} \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

commutes, where π is the canonical projection.

(2) For any homomorphism $\varphi : G \to H$ and $n \geq 1$, we have $\varphi(G^{(n)}) \subset H^{(n)}$ and if φ is surjective, $\varphi(G^{(n)}) = H^{(n)}$.

(3) $G^{(n)}$ is a characteristic subgroup of G.

<u>Proof</u>: (1) Let $\pi : G \to G_{ab}$ be the canonical projection. Let $x, y \in G_{ab}$, and $g, h \in G$ with $\pi(g) = x$, $\pi(h) = y$. Then $xyx^{-1}y^{-1} = [x, y] = [\pi(g), \pi(h)]$

$$= \pi([g, h])$$

But $[g,h] \in G^{(1)} = \operatorname{Ker} \pi$, hence

$xyx^{-1}y^{-1} = e$, that is, $xy = yx$.

Since A is abelian we have

for every $(x_1, y_1, \ldots, x_r; y_r) \in G^{2r}$:

$$\varphi\left(\prod_{i=1}^{r} [x_i, y_i]\right) = \prod_{i=1}^{r} [\varphi(x_i), \varphi(y_i)] = e.$$

Hence $G^{(1)} \subset \operatorname{Ker} \varphi$.

Thus φ factors as follows:

$$\begin{tikzcd}
G \arrow[d, "\pi"'] \arrow[drr, "\varphi"] & & \\
G_{ab} = G/G^{(1)} \arrow[d, "p"'] & & A \\
G/_{\operatorname{Ker}\varphi} \arrow[urr, "\tilde{\varphi}"'] & &
\end{tikzcd}$$

Now define $\bar{\varphi} := \tilde{\varphi} \circ p$.

(2) We have as above for $(x_1, y_1, \ldots, x_r, y_r) \in G^{2r}$: $\varphi(\prod [x_i, y_i]) = \prod [\varphi(x_i), \varphi(y_i)]$

thus $\varphi(G^{(1)}) \subset H^{(1)}$ and by recurrence

$$\varphi(G^{(n)}) = \varphi((G^{(n-1)})^{(1)}) \subset \varphi(G^{(n-1)})^{(1)}$$

$$\subset (H^{(n-1)})^{(1)} = H^{(n)}.$$

The rest is clear. ☒

Def. III. 13

G is solvable if there exists a sequence

$$G = G_0 \triangleright G_1 \triangleright G_2 \cdots \triangleright G_n = (e)$$

of subgroups s.t.

(1) $G_{i+1} \triangleleft G_i \qquad 0 \leq i \leq n-1$

(2) G_i / G_{i+1} is abelian.

Remark III. 14. In the context of lemma III. 9

$Gal(K_t / k)$ is solvable.

The next lemma gives a kind of procedure to check when a group is solvable:

Lemma III. 15 : The following are equivalent

(1) G is solvable

(2) there is $n \geq 1$ such that $G^{(n)} = (e)$.

<u>Proof</u>: (2) $\Rightarrow$ (1) is clear.

(1) $\Rightarrow$ (2):

Since G_i / G_{i+1} is abelian, we have

$$G_i^{(1)} \subset G_{i+1} ;$$

thus $G^{(1)} \subset G_1$, $G^{(2)} = [G^{(1)}, G^{(1)}] \subset G_2$

and by recurrence $G^{(n)} \subset G_n = \{e\}$.

$\boxed{\xi}$

<u>Examples III.16</u>

(1) S_2, S_3, S_4 are solvable (exercise).

S_5 is not: $[S_5, S_5] = A_5$, and since

A_5 is simple non-abelian,

$$[A_5, A_5] = A_5 .$$

Thus the derived series stops at A_5.