22. 4. 24.

Thm 3.6. Let $\chi_1, \ldots \chi_n$ be distinct characters of a gp G with values in a field L. Then they are lin indep over L.

Proof Suppose on the contrary they're lin dependent. Among all linear dependence relations choose one with minimal number of non-zero coefs. By renumbering if necessary assume the non-zero coefs are $a_1, \ldots a_m$, $1 < m \leq n$ and

$$a_1 \chi_1 + \ldots + a_m \chi_m = 0$$

Then $\forall g \in G$, $a_1 \chi_1(g) + \ldots + a_m \chi_m(g) = 0$. ①

Let g_0 be an elt of G s.t $\chi_1(g_0) \neq \chi_m(g_0)$. Such g_0 exists since $\chi_1 \neq \chi_m$

Since ① holds for any $g \in G$, it also holds for gg_0 and we have

$$a_1 \chi_1(gg_0) + \ldots + a_m \chi_m(gg_0) = 0$$

$$0 = a_1 \chi_1(g) \chi_1(g_0) + \ldots + a_m \chi_m(g) \chi_m(g_0). \quad ②$$

Multiplying eqn 1 with $\chi_m(g_0)$ and subtracting from 2 we get $\forall g \in G$

$$a_1 \chi_1(g)\left[\chi_m(g_0) - \chi_1(g_0)\right] + \cdots +$$

$$a_{m-1}\chi_{m-1}(g)\left[\chi_m(g_0) - \chi_{m-1}(g_0)\right] = 0 \quad (3)$$

By choice of g_0, $\chi_m(g_0) - \chi_1(g_0) \neq 0$

Hence (3) is a lin. dependence relation with fewer than m non-zero coefs contradicting the minimality of m $\square$

As a corollary we get

Thm 3.7 let $\sigma_1, \ldots, \sigma_n$ be distinct monomorphisms (embeddings) of a field K into L. Then they are lin. independent over L as functions on K. In particular distinct autom. of a field K are lin. indep as functions on K.

Proof. Consider any injective hom $\sigma: K \to L$. Then in particular σ is a hom of multiplicative group $G = K^\times$ into the multip. gp $L^\times$ (Since $\sigma(0)=0$, and σ is injective $\sigma(K^\times) \subset L^\times$)

Hence σ may be viewed as a character of $K^\times$ with values in L

Note σ contains all necessary information about σ as a function on K since only pt not considered by $\sigma : K^\times \longrightarrow L^\times$ is 0 and $\sigma(0) = 0$.

$\boxtimes$

Our next main result, which will lead us to a relationship between the degree of an extension $[L : K]$ and the size of its Galois group $\mathrm{Gal}(L : K)$, is the following

Thm 5.8 Let L be a field, $G \leq \mathrm{Aut}(L)$ a finite subgroup of $\mathrm{Aut}(L)$.
Let $L_0 := \text{Fix field of } G = L^G = \phi(G)$
Then
$$[L : L_0] = [L : L^G] = |G| .$$

Proof Recall 2 simple lemmas, one from linear algebra

Lemma 1 If $n > m$ then a system of m homog. eqns in n unknowns
$$a_{i1} x_1 + \cdots + a_{in} x_n = 0 \qquad i = 1, \ldots, m$$

with coefs taken from a field L has a non-trivial soln, $x_1 \ldots x_n \in L$.

The second from group theory

<u>lemma 2</u> Let G be a gp, $g_0 \in G$ then $\{g g_0\}_{g \in G} = G$.

Now let $G = \{\sigma_1 \ldots \sigma_n\} \leq Aut(L)$
and
$$L_0 = L^G = Fix(G).$$

(1) First suppose $[L : L^G] = m < n = |G|$

Fix a basis $\{\omega_1, \ldots \omega_m\}$ of L over $L_0 = L^G$
Consider the system of hom. eqns in y's

$$(1) \quad \sigma_1(\omega_j) y_1 + \ldots + \sigma_n(\omega_j) y_n = 0 \qquad j = 1, \ldots m.$$

There are more unknowns, n, than # of eqns, m. Hence by lemma 1 $\exists$ y_i's in L, not all zero, satisfying.

$$(y_1 \sigma_1 + \ldots + y_n \sigma_n)(\omega_j) = 0 \qquad j = 1, \ldots, m$$

Hence the autom $y_1\sigma_1 + \ldots + y_n\sigma_n = 0$ on a basis of L over L_0.

Let a be any element of L. Then

$$a = a_1 w_1 + \dots + a_m w_m \quad \text{with } a_i \in L_0 = \text{Fix}(G$$

ie $\sigma(a_\ell) = a_\ell \quad \ell = 1, \dots, m$

Then $(y_1\sigma_1 + \dots + y_n\sigma_n)(a) = (y_1\sigma_1 + \dots + y_n\sigma_n)\left(\sum_{\ell=1}^{m} a_\ell w_\ell\right.$

$$= \sum_{\ell=1}^{m} a_\ell \underbrace{(y_1\sigma_1 + \dots + y_n\sigma_n)(w_\ell)}_{=0 \text{ by } (1)} = 0$$

Hence $(y_1\sigma_1 + \dots y_n\sigma_n)(a) = 0 \quad \forall\, a \in L$

$\Rightarrow \sigma_1 \dots \sigma_n$ are lin. dep $\lightning$

Hence $[L : L_0] \geq n$.

Now suppose $[L : L_0] > n$. Then $\exists\ n+1$ elements of L that are lin. indep over L_0. Let $\{w_1, \dots w_{n+1}\}$ be such a set.

Consider the homog sys. of eqns

(2) $\sigma_j(w_1)y_1 + \dots + \sigma_j(w_{n+1})y_{n+1} = 0 \quad j = 1, \dots, n$

The system (2) has more unknowns $n+1$, than equations, n.

Hence again by lemma 1, $\exists\ y_1 \dots y_{n+1} \in L$ not all zero which satisfy (2).

Choose a soln $y_1, \dots y_{n+1}$ so that as few of them as possible are non-zero, renumber so that $y_1, \dots y_r \neq 0$, $y_{r+1}, \dots y_{n+1} = 0$

Hence (2) becomes

(3) $\sigma_j(w_1)y_1 + \dots + \sigma_j(w_r)y_r = 0 \qquad j = 1, \dots n$

Let $\sigma \in G$. Apply σ to (3) to get

(4) $\sigma\sigma_j(w_1)\sigma(y_1) + \dots \sigma\sigma_j(w_r)\sigma(y_r) = 0$
$j = 1, \dots n$

Since $\{\sigma_j\}_j$ run over G
so does $\{\sigma\sigma_j\}_j$

Let $\sigma\sigma_j = \sigma_\ell$ as j runs over $1, \dots, n$
so does ℓ.

Hence (4) can be written as

(5) $\sigma_\ell(w_1)\sigma(y_1) + \dots + \sigma_\ell(w_r)\sigma(y_r) = 0 \quad \ell = 1, \dots n$

Recall (3) from above

(3) $\sigma_\ell(w_1)y_1 + \dots + \sigma_\ell(w_r)y_r = 0 \qquad \ell = 1, \dots n.$

Multiply (5) with y_1
(3) with $\sigma(y_1)$ and subtract

to get $\sigma_\ell(w_2)\sigma(y_2)y_1 + \dots + \sigma_\ell(w_r)\sigma(y_r)y_1$

$- \sigma_\ell(w_2)\sigma(y_1)y_2 + \dots + \sigma_\ell(w_r)\sigma(y_1)y_r$

$= \sigma_\ell(w_2)[\sigma(y_2)y_1 - \sigma(y_1)y_2] + \dots +$

$\sigma_\ell(w_r)[\sigma(y_r)y_1 - \sigma(y_1)y_r] = 0. \quad (6)$

(6) is a system like (3) with $r-1 < r$ terms.

This would be a contradiction to minimality of r unless

$$\sigma(y_1)y_\ell = \sigma(y_\ell)y_1 \qquad \ell = 2, \dots r.$$

If this happens then $y_\ell y_1^{-1} = \sigma(y_\ell y_1^{-1})$

$\forall \sigma \in G.$

$\Rightarrow \quad y_\ell y_1^{-1} \in Fix(G) = L_0 \qquad \ell = 1, \dots r.$

Hence $\exists$ $z_1, \dots z_r \in L_0$ and $0 \neq k (= y_1) \in L$ s.t

$$y_\ell = k z_\ell \qquad \ell = 1, \dots r.$$

Putting this in (3) and taking $\sigma =$ identity

ie.

(3) $\sigma_j(w_1)y_1 + \cdots + \sigma_j(w_r)y_r = 0$

gives $w_1(kz_1) + \cdots + w_r(kz_r) = 0$

Since $k \neq 0$ we get $w_1 z_1 + \cdots + w_r z_r = 0$

with $z_i \in L_0$, $z_i \neq 0$. Hence we get

$\{w_1 \ldots w_r\}$ are lin dep. over L_0

which is a contradiction.

Hence $[L : L_0] = |G| = n$.

∎

We now look at some immediate corollaries of Thm 3.8.

We've seen that if L is a splitting field of a poly f then $|Gal(L:K)| \leq [L:K]$ with equality if f is separable.