[redacted]

Character theory

Def^{n}: A L-character of a gp. G is a hom.

$$\chi : G \to L^{\times}.$$

Th^{m} If ~~$\chi_1, \dots \chi_n$ are~~ distinct characters are linearly independent

pf: If not, among linear dependencies, pick one with the minimal # of nonzero coefficients.

Say $\sum_{i=1}^{m} a_i \chi_i = 0$ (as $\mathbb{R}$-fn)

That is, $\sum a_i \chi_i(g) = 0 \quad \forall g \in G.$

e the characters are distinct, $\exists\ g_0 \in G$, $\chi_1(g_0) \neq \chi_m(g_0)$.

Thus, $\forall g \in G$, $\sum a_i \chi_i(g_0 g) = \sum a_i \chi_i(g_0)\chi_i(g) = 0$.

$\Rightarrow$ Also, $\sum a_i \chi_i(g) = 0 \Rightarrow \sum a_i \chi_i(g)\chi_m(g_0) = 0$.

Subtracting, $a_1 \chi_1(g_0)\chi_1(g) + \cdots + a_m \chi_m(g_0)\chi_m(g)$
$- (a_1 \chi_m(g_0)\chi_1(g) + \cdots + a_m \chi_m(g_0)\chi_m(g)) = 0$
$= \sum_{i=1}^{m-1} a_i [\chi_i(g_0) - \chi_m(g_0)]\chi_i(g) = 0$.
$(\forall g \in G)$.

Thus, But χ_m the leading coeff is nonzero
Contradicting the minimal length of the linear dependence

Embeddings $K \hookrightarrow L$ also give homs $K^\times \to L^\times$,
so are L-characters of $K^\times$. Contains all important info
(who cares about 0?!)

Cor: If $\sigma_1, \ldots, \sigma_n$ are distinct embeddings of $K \hookrightarrow L$,
then they are K-linearly independent

For example, distinct automorphisms of K are K-lin. ind.
$= \{\sigma_1, \ldots \sigma_n\}$

Theorem: If. $G \leq \mathrm{Aut}(K)$, $F := \mathrm{Fix}(G)$, then
$[K:F] = n = |G|$

Pf: If $n > [K:F] = m$. Then take an F-basis of K: $\{\omega_1, \ldots, \omega_m\}$.
Consider the system:

$$\sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n = 0$$
$$\vdots$$
$$\sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n = 0.$$

unknowns $>$ # eqns $\Rightarrow \exists$ nontrivial sol $= \beta_1, \ldots, \beta_n$

Pick any m elts. $a_1, \dots, a_m \in F$.

Then all the σ_i fix F, so multiplying the i-th eqn by a_i

$$\rightsquigarrow \quad \sigma_1(a_1\omega_1)\beta_1 + \cdots + \sigma_n(a_1\omega_1)\beta_n = 0$$
$$\vdots$$
$$\sigma_1(a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_m\omega_m)\beta_n = 0.$$

Add these eqns all together $\rightsquigarrow$

$$\sigma_1\left(\textstyle\sum a_i\omega_i\right)\beta_1 + \cdots + \sigma_n\left(\sum a_i\omega_i\right)\beta_n = 0.$$

But $a_i \in F$ were arbitrary, so every F-linear comb. of ω_i z gives $\sum \sigma_i(z)\beta_i = 0$. As $\{\omega_i\}$ is a basis of K,

$$\sum \sigma_i(k)\beta_i = 0 \ \forall k \in K \iff \sum \sigma_\ell \beta_i \sigma_j = 0$$

as fns

$\Rightarrow$ the σ_i are linearly dependent. (contradicts Thm) $n \le [K:F]$. Suppose $n < [K:F]$ (last corollary). Then there are more than n F-lin. independent elts of F, including $\alpha_1, \dots, \alpha_{n+1}$. Consider now the system

$$\sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} = 0$$
$$\vdots$$
$$\sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} = 0.$$

unknowns > # eqns $\Rightarrow \exists$ sol'n $\beta_1, \dots, \beta_{n+1} \in K$ not all 0.

If all the β_i are really in F, then since $\sigma_1 = \mathrm{id}_K$, we'd have a contradiction to the F-linear independence of the α_i.

Choose a set of sol'ns $\{\beta_i\}$ with the minimal

we assume all $\beta_i \neq 0$. Can also divide them by β_r so $\beta_r = 1$.

WLOG, say $\beta_1 \notin F$. Then we get

$$\sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) = 0$$
$$\vdots$$
$$\sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) = 0,$$

As $\beta_1 \notin F$, there is an automorphism σ_k with $\sigma_k(\beta_1) \neq \beta_1$. ($F$ = fixed field)

Applying σ_k to all these eqns gives:

$$\sigma_k(\sigma_1(\alpha_1))\,\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_1(\alpha_{r-1})\,\sigma_k(\beta_{r-1}) + \sigma_k\sigma_1(\alpha_r) = 0$$
$$\vdots$$
$$\sigma_k(\sigma_n(\alpha_1))\,\sigma_k(\beta_1) + \cdots + \sigma_k\sigma_n(\alpha_r) = 0.$$

As $\{\sigma_i\}$ is a group, $\{\sigma_k\sigma_i\} = \{\sigma_i\}$ (just a permutation)

Thus, if $\sigma_i := \sigma_k \circ \sigma_i$, we get the system of eqns

$$\left\{\sigma_i(\alpha_1)\,\sigma_k(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\,\sigma_k(\beta_{r-1}) + \sigma_i(\alpha_r) = 0\right\}_{i=1}^{n}$$

Previously, we had the system

$$\left\{\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_r) = 0\right\}_{i=1}^{n}.$$

Subtracting these two gives

$$\sigma_i(\alpha_1)\left[\beta_1 - \sigma_k(\beta_1)\right] + \cdots + \sigma_i(\alpha_{r-1})\left[\beta_{r-1} - \sigma_k(\beta_{r-1})\right] = 0.$$

Not $= 0$ & $\neq 0$ and thus gives a smaller

System with fewer than r nonzero x_i

Cor K/F finite $\Rightarrow |\mathrm{Aut}(K/F)| \le [K:F]$.

Equality $\Leftrightarrow F =$ fixed field of $\mathrm{Aut}(K/F)$.

That is, K/F Galois iff $F =$ fixed field of $\mathrm{Aut}(K/F)$.

Pf: Call F_1 to be the fixed field of K/F.

By the th^m, $[K:F_1] = |\mathrm{Aut}(K/F)|$

$\Rightarrow [K:F] = |\mathrm{Aut}(K/F)| \cdot |F_1:F|$.

Cor: Let $G \le \mathrm{Aut}(K)$ and $F = \mathrm{Fix}(G)$.

Then every F-aut. of K is contained in G

so that K/F is Galois with Galois gp. G.

Pf: G fixes everything in F by defn

$\Rightarrow G \le \mathrm{Aut}(K/F) \Rightarrow |G| \le |\mathrm{Aut}(K/F)|$.

The theorem says $|G| = [K:F]$, so

$[K:F] \le |\mathrm{Aut}(K/F)|$. But $[K:F] \overset{(Cor)}{\ge} |\mathrm{Aut}(K/F)|$

So $[K:F] = |G| \le |\mathrm{Aut}(K/F)| \le [K:F]$

$\Rightarrow$ all equalities.

Cor: Fixed fields of distinct subgps of $\mathrm{Aut}(K)$ are distinct ($H_1 \ne H_2$).

pf: If $F_1 = \mathrm{Fix}(G_1)$, $F_2 = \mathrm{Fix}(G_2)$, $G_i \le \mathrm{Aut}(K)$. If $F_1 = F_2$,