Back to 562

Where next?

① (more) Galois Theory & Applications

② Polynomials in $\geq 2$ variables (if time...).

---

The Galois Group:

Given a field extension $\mathbb{Q} \subseteq F \subseteq K$, consider the group

$$\mathrm{Gal}(K/L) := \{ \text{field automorphisms } \sigma : K \to K \text{ s.t. } \sigma(a) = a \ \forall\, a \in F \}.$$

Prototype: Define $\sigma : \mathbb{C} \to \mathbb{C}$ by
$\sigma(a + ib) := a - ib$.

Then
$$\left.\begin{aligned} \sigma(\alpha\beta) &= \sigma(\alpha\beta) \\ \sigma(\alpha+\beta) &= \sigma(\alpha) + \sigma(\beta) \end{aligned}\right\} \ \forall\, \alpha, \beta \in \mathbb{C}.$$
($\sigma$ is a field automorphism)

And $\sigma(\alpha) = \alpha \quad \forall\, \alpha \in \mathbb{R}$

$\Rightarrow \quad \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

Are there any more?

Suppose $\mu \in Gal(\mathbb{C}/\mathbb{R})$. Then $\mu$ is completely determined by the value $\mu(i) \in \mathbb{C}$ since $\mu(a+ib) = \mu(a) + \mu(i)\mu(b)$
$= a + \mu(i) b$.

(Reason: $1, i$ is a basis for $\mathbb{C}/\mathbb{R}$).

So what could $\mu(i)$ be?
$\forall z \in \mathbb{C}$ we have

$$\mu(z^2+1) = \mu(z)^2 + \mu(1) = \mu(z)^2 + 1.$$

Also note $\mu(w) = 0 \iff w = 0$.
<u>Proof</u>: Apply $\mu^{-1}$ to get $w = \mu^{-1}(0) = 0$. $\boxtimes$
hom.

Corollary: $\forall z \in \mathbb{C}$, $\mu \in Gal(\mathbb{C}/\mathbb{R})$.

$$z^2 + 1 = 0 \iff (\mu(z))^2 + 1 = 0.$$

($\mu$ permutes the roots of $x^2+1$).

There are exactly 2 choices:

$$\mu = \begin{Bmatrix} i \mapsto i \\ -i \mapsto -i \end{Bmatrix} \qquad \mu = \begin{Bmatrix} i \mapsto -i \\ -i \mapsto i \end{Bmatrix}.$$

id. complex conjugation $\sigma$.

Theorem: $Gal(\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$

Table:

$$\begin{array}{c|cc} \circ & id & \sigma \\ \hline id & id & \sigma \\ \sigma & \sigma & id \end{array} \approx \mathbb{Z}/(2)$$

Useful Observations: Given $\mathbb{Q} \subseteq F \subseteq K$

1. $\mu \in Gal(K/F)$ is determined by its values on a generating set, say $K = F(a_1, a_2, \ldots, a_n)$

2. If $\mu \in Gal(K/F)$ and $f(x) \in F[x]$ then $\mu$ permutes the roots of $f(x)$ in $K$

Proof: $\forall \alpha \in K$ we have $\mu(f(\alpha)) = f(\mu(\alpha))$.
Hence $f(\alpha) = 0 \iff \mu(f(\alpha)) = 0$
$\iff f(\mu(\alpha)) = 0$ $\blacksquare$

HW 5 due Wed Apr 11.

Exam 2 stats.

| | | |
|---|---|---|
| Total | 19 | $A \approx 11$ and above |
| Mean | 12 | $B \approx 10$ and below. |
| Median | 11 | |
| St. Dev. | 4.5 | |

Recall: $Gal(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$ where.

$\sigma(a+ib) = a-ib$.

How did we prove it?

Let $\mu \in Gal(\mathbb{C}/\mathbb{R})$. Then $\mu$ is determined by $\mu(i)$ (since $\mathbb{C} = \mathbb{R}(i)$)

Look at minpoly $x^2+1 \in \mathbb{Q}[x]$ of $i \in \mathbb{C}$.

$\forall z \in \mathbb{C}$ we have

$$z^2+1=0 \iff \mu(z^2+1)=0$$
$$\iff (\mu(z))^2+1=0$$

Conclusion: $\mu$ permutes the roots of $x^2+1$

There are exactly 2 choices :

$$\mu = \left\{ \begin{matrix} i \to i \\ -i \to -i \end{matrix} \right\}, \quad \mu = \left\{ \begin{matrix} i \to -i \\ -i \to i \end{matrix} \right\}$$

$\mathbb{1}$ $\qquad$ $\sigma$ "complex conjugation".

Useful Observations : Given $F \subseteq K \subseteq L$ suppose $K = F(a_1, a_2, \ldots, a_n)$ for some $a_1, a_2, \ldots, a_n \in L$.

(1) $\mu \in Gal(K/F)$ is determined by the values $\mu(a_1), \ldots, \mu(a_n) \in K$.

Proof : By the Tower Law, $K/F$ has a basis of monomials in the $a_i$'s.

( e.g. $2a_1^3 a_2^5 a_6^7 + 3a_5^2 a_9$ ). ///

Q : Are there further restrictions on $\mu \in Gal(K/F)$?

(2) If $f(x) \in F[x]$ then $\mu$ permutes the roots of $f(x)$ in $K$.

Proof : $\forall \alpha \in K$ we have $\mu(f(\alpha)) = f(\mu(\alpha))$.

Hence

$f(\alpha) = 0 \iff \mu(f(\alpha)) = 0 \iff f(\mu(\alpha)) = 0$.

" $\alpha$ is a root $\iff$ $\mu(\alpha)$ is a root " ///.

Corollary: If $K/F$ is algebraic, then
$$|Gal(K/F)| < \infty.$$

Proof: For simplicity let's say $\mathbb{Q} \subseteq F$.
Then $K = F(\alpha)$ for some algebraic $\alpha \in \mathbb{C}$.
(Steinitz, I.O.U.)
Let $m_\alpha(x) \in F[x]$ be the minpoly, say

$$[K:F] = \deg m_\alpha(x) = n$$

Then $\mu \in Gal(K/F)$ is determined by $\mu(\alpha)$, and $\mu(\alpha) \in K$ is a root of $m_\alpha(x)$.
Since $m_\alpha(x)$ has $\leq n$ roots we get

$$|Gal(K/F)| \leq n = [K:F] \qquad \boxtimes$$

We have shown

Theorem: For algebraic $\mathbb{Q} \subseteq F \subseteq K$ we have
$$|Gal(K/F)| \leq [K:F].$$

Q: When do we get $=$ ?

A: If $K = F(\alpha)$ and $K$ contains <u>all</u> the roots of $m_\alpha(x)$ then

$$|Gal(K/F)| = [K:F]$$

<u>Proof</u>: Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ be the roots of $m_\alpha(x)$, and let $\mu \in Gal(K/F)$. Then $\mu(\alpha) = \alpha_i$ for some $i \in 1, \ldots, n$ and this determines $\mu$. Every choice is <u>possible</u> because $\forall\, i$,

$\exists \mu$. Call this map $\mu_i : K \to K$.

$$K = F(\alpha) \overset{\sim}{\longleftrightarrow} \frac{F[x]}{(m_\alpha(x))} \overset{\sim}{\longleftrightarrow} F(\alpha_i) = K$$

$$\begin{array}{ccccc} f(\alpha) & \longleftarrow\!\shortmid & f(x) + (m_\alpha(x)) & \shortmid\!\longrightarrow & f(\alpha_i) \\ a & \longleftarrow\!\shortmid & a + (m_\alpha(x)) & \shortmid\!\longrightarrow & a \end{array}$$

Then $\mu_i : K \to K$ is an automorphism,

$\mu_i(a) = a \ \forall\, a \in F$.

$\mu_i(\alpha) = \alpha_i$

Hence $Gal(K/F) = \{\mu_1, \mu_2, \ldots, \mu_n\}$

and $|Gal(K/F)| = n = [K:F]$ ∎

HW 5 due Wed Apr 11.

Today: Steinitz' Theorem $F(a,b) = F(c)$.
(The Main Lemma of Galois Theory)

Def: Given $f(x) = \sum_{k \geq 0} a_k x^k \in F[x]$,
define its formal derivative

$$f'(x) := \sum_{k \geq 1} k a_k x^{k-1} \in F[x].$$

$$\left( k a_k = \underbrace{a_k + a_k + \cdots + a_k}_{k \text{ times}} \right).$$

Lemma: $\forall f(x), g(x) \in F[x]$, $a \in F$,

- $(f(x) + g(x))' = f'(x) + g'(x)$
- $(a f(x))' = a f'(x)$

"linear"

- $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$ (Leibniz rule).

Proof: see Calc I ☒

Next Issue: Repeated roots.

Q: When does an irreducible polynomial $\in F[x]$ have a repeated root?
(where? in some field extension)

Lemma: $f(x) \in F[x]$ has a repeated root (in some extension) $\iff$ $f(x), f'(x)$ are not coprime in $F[x]$.

Proof: "$\Longrightarrow$" Consider $F \subseteq K$ with $a \in K$, $g(x) \in K[x]$ and $f(x) = (x-a)^2 g(x) \in K[x]$. Then in $K$ we have

$$f'(x) = (x-a)^2 g'(x) + 2(x-a) g(x) \in K[x]$$

$\Longrightarrow f'(a) = 0 \Longrightarrow f, f'$ have common factor $(x-a)$ in $K[x]$.

☆ If $f, f'$ coprime in $F[x]$, $\exists\, h, k \in F[x]$ with $f(x)h(x) + f'(x)k(x) = 1$
Viewing this equation over $K$ gives $(x-a) \mid 1$ in $K[x]$. Contradiction ✗

"$\Longleftarrow$" Say $f, f'$ have gcd $g(x) \in F[x]$. and consider $a \in K \supseteq F$ with $g(a) = 0$ ($\exists$ by Kronecker), hence $f(a) = f'(a) = 0$.

☆ If $f$ has no repeated roots then $\exists\, q(x) \in K[x]$ with $f(x) = (x-a)q(x)$ and $q(a) \neq 0$.
Finally,

$$f'(x) = (x-a)q'(x) + q(x)$$

$\Longrightarrow q(a) = f'(a) = 0$ ✗ $\boxtimes$

Corollary: Let $\mathbb{Q} \subseteq F$ and let $f(x) \in F[x]$ be irreducible. Then $f$ has no repeated root in any extension.

Proof: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ be irred / $F$ and suppose it has a multiple root. By Lemma $\Rightarrow$ $f, f'$ not coprime.
$\Rightarrow f(x) \mid f'(x)$. But $\deg(f') = n-1$.
$\Rightarrow f'(x) \equiv 0$.

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \equiv 0$$

$$\Rightarrow n a_n = (n-1) a_{n-1} = \cdots = 2a_2 = a_1 = 0$$

char 0 $\Rightarrow a_n = a_{n-1} = \cdots = a_2 = a_1 = 0$

$\Rightarrow f(x) = a_0 \in F$. Contradiction

[Remark: Let $f(x) \in F[x]$ be irred with a multiple root somewhere. If char $F = p$ then $f(x) = g(x^p)$ for some $g(x) \in F[x]$.
$\Rightarrow$ all roots have the same multiplicity]

Finally,

**Primitive Element Theorem** (Steinitz, 1910):
Consider $\mathbb{Q} \subseteq F \subseteq K$ with $a, b \in K$ algebraic over $F$. Then $\exists\, c \in K$ with

$$F(a,b) = F(c)$$

Proof: Let $A(x), B(x) \in F[x]$ be minpolys for $a, b$.
Let $a = a_1, a_2, \dots, a_m$ $(\in \mathbb{C})$ be the roots of $A(x)$
Let $b = b_1, b_2, \dots, b_n$ $(\in \mathbb{C})$ be the roots of $B(x)$.
Since $|F| = \infty$ $\exists$ $d \in F$ such that

$$d \neq (a_i - a)/(b - b_j) \quad \forall\, i \geq 1,\ j > 1.$$
$$\left( a_i \neq a + d(b - b_j) \quad \forall\, i \geq 1,\ j > 1 \right).$$

Let $c = a + db$. Claim: $F(a,b) = F(c)$.
Well $c \in F(a,b) \Rightarrow F(c) \subseteq F(a,b)$.
Want to show $a, b \in F(c)$ (hence $F(a,b) \subseteq F(c)$)
Suffices to show $b \in F(c)$. (why?)

Define $h(x) = A(c - dx) \in F(c)[x]$ and observe that

$$h(b_1) = A(c - db_1) = A(a_1) = 0.$$
$$h(b_j) = A(\underbrace{c - db_j}_{\neq \text{ any } a_i}) \neq 0 \quad \forall j > 1.$$

Hence $b = b_1$ is the only common root of $h(x), B(x) \in F(c)[x]$.

Let $m_b(x) \in F(c)[x]$ be the minpoly of $b / F(c)$.
$\Longrightarrow m_b \mid h$, $m_b \mid B$ in $F(c)[x]$.

Sp. $\deg(m_b) \geq 2$. Since $B$ has no repeated roots (by Lemma), then $h, B$ have $\geq 2$ distinct roots in common (i.e. the roots of $m_b$). $\times$.

Hence $\deg(m_b) = 1$
$\Longrightarrow m_b(x) = x - b \in F(c)$
$\Longrightarrow b \in F(c)$

$\blacksquare$

HW5 due next Wed.

Today: "Symmetric" Polynomials
(Glimpse of polys in $\geq 2$ variables)

Recall we can define $R[x]$ for any ring $R$, and $R[x]$ inherits some properties from $R$:

- $R$ domain $\Rightarrow$ $R[x]$ domain
- $R$ Euclidean $\not\Rightarrow$ $R[x]$ Euclidean
- $R$ PID $\not\Rightarrow$ $R[x]$ PID
- However,

$$\boxed{R \text{ UFD} \Rightarrow R[x] \text{ UFD}}$$ proof omitted.

(Gauss showed this for $R = \mathbb{Z}$)

Interesting case: $R = \overset{\text{UFD}}{F[y]}$. Then

$$F[y][x] = \Big\{ \sum_{k \geq 0} f_k(y) x^k : \underset{\text{almost all zero.}}{f_k(y) \in F[y]} \Big\}$$

$$= \Big\{ \sum_k \Big( \sum_l a_{kl} y^l \Big) x^k : \underset{\text{almost all zero}}{a_{kl} \in F} \Big\}$$

$$= \Big\{ \sum_{k,l \geq 0} a_{kl} x^k y^l : a_{kl} \in F \text{ almost all zero} \Big\}$$

$$=: F[x,y] \quad \text{(it's a UFD)}.$$

If $x, y$ algebraically independent

i.e. $\sum_{k,l} a_{kl} x^k y^l = 0 \iff a_{kl} = 0 \ \forall k, l.$

Then $F[x,y]$ is called the ring of polynomials in 2 variables $x, y$.

By induction define

$$F[x_1, x_2, \dots, x_n] = \{ \sum_\alpha a_\alpha x^\alpha : a_\alpha \in F \text{ almost all zero} \}$$

where $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$ is a multi-index and $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. (called a monomial).

If $x_1, \dots, x_n$ are transcendental and alg. ind. over $F$, we call them "variables".

[ Remark: It is not known whether $\pi, e$ are alg. ind. over $\mathbb{Q}$.

i.e. $\mathbb{Q}[\pi, e] \overset{?}{\approx} \mathbb{Q}[x_1, x_2]$

However $\mathbb{Q}[\pi, e^\pi] \approx \mathbb{Q}[x_1, x_2]$ is known, apparently ]

Let $S_n = \mathrm{Aut}(\{1,2,\dots,n\})$
$= $ group of permutations $\{1,2,\dots,n\} \to \{1,2,\dots,n\}$
$=$ the "symmetric group".

$|S_n| = n!$

Then $S_n$ <u>acts on</u> $F[x_1,\dots,x_n] = R$ permuting variables. Given $\sigma \in S_n$, $f = f(x_1,\dots,x_n)$ we define

$$\sigma \circ f := f(x_{\sigma(1)},\dots,x_{\sigma(n)}).$$

Let $R^{S_n} := \{f \in R : \sigma \cdot f = f \ \forall \sigma \in S_n\} \subseteq R$.

In fact, $R^{S_n}$ is a subring of $R$, called the ring of symmetric polynomials

eg. $x^3 + y^3 + z^3 \in F[x,y,z]^{S_3}$

The study of $R^{S_n}$ goes back to Isaac Newton.

Why did he care?

Let $R = F[x_1, \ldots, x_n]$ and consider $R[t]$.
We define the <u>elementary</u> <u>symmetric</u> <u>polys.</u> by.

$$t^n - e_1 t^{n-1} + e_2 t^{n-2} - \cdots + (-1)^n e_n t^0$$
$$:= (t - x_1)(t - x_2) \cdots (t - x_n).$$

So. $e_1 = x_1 + x_2 + \cdots + x_n$

$e_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n = \sum_{1 \le i < j \le n} x_i x_j$

$\vdots$

$e_n = x_1 x_2 \cdots x_n$

By definition, $e_1, e_2, \ldots, e_n \in R^{S_n}$.

<u>Newton's</u> <u>Theorem</u>:

$$R^{S_n} \approx F[e_1, \ldots, e_n]$$

i.e. The evaluation map.

$$\varphi_{e_1, \ldots, e_n} : F[x_1, \ldots, x_n] \longrightarrow R^{S_n}$$
$$f(x_1, \ldots, x_n) \longmapsto \text{"} f(e_1, \ldots, e_n) \text{"}$$

is an <u>isomorphism</u> of rings

Ex. $x^3 + y^3 + z^3 \overset{?}{\in} F[e_1, e_2, e_3]$

Order degree sequences lexicographically

eg $\underset{1}{(0,0,0)} < \underset{z}{(0,0,1)} < \underset{y}{(0,1,0)} < \underset{yz^2}{(0,1,2)}$

Underline the leading term and then kill it.

$$\underline{x^3} + y^3 + z^3 - (x+y+z)^3$$
$$- (\underline{x^3} + y^3 + z^3 + 3x^2y + 3xy^2 + 3x^2z + 3xz^2 + 3y^2z + 3yz^2 + 6xyz)$$

$$x^3 + y^3 + z^3 - e_1^3 = \underline{-3x^2y} + \text{lower order terms.}$$

Now add $3e_1e_2$

$$3e_1e_2 = 3(x+y+z)(xy+xz+yz)$$
$$= 3(x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2 + 3xyz)$$

$$x^3 + y^3 + z^3 - e_1^3 + 3e_1e_2 = \underline{3xyz} = 3e_3 \quad \checkmark$$

$$x^3 + y^3 + z^3 = e_1^3 - 3e_1e_2 + 3e_3$$

i.e. $\varphi_{e_1,e_2,e_3} : F[x,y,z] \to F[x,y,z]^{S_3}$

$$x^3 - 3xy + 3z \mapsto x^3 + y^3 + z^3.$$

In general, let

$$p_k(x_1, \dots, x_n) = x_1^k + \cdots + x_n^k$$

power sum symm. polys.

Then Newton proved.

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_k \quad \forall k.$$

(Newton-Girard Formula)

$\Longrightarrow$ $p_1 = e_1$

$p_2 = e_1 p_1 - 2e_2$

$p_3 = e_1 p_2 - e_2 p_1 + 3e_3$

$\vdots$

etc.

HW 5 due Wed.

Today: Symm. Polys. $\rightsquigarrow$ Galois

Recall: The elementary symm. polys $e_1, e_2, \ldots, e_n \in F[x_1, \ldots, x_n]$ are defined by

$$t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n t^0 = (t-x_1)(t-x_2)\cdots(t-x_n)$$

i.e. $e_1 = x_1 + x_2 + \cdots + x_n$ (trace)

$\vdots$

$$e_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le n} x_{i_1} x_{i_2} \cdots x_{i_r}$$

$e_n = x_1 x_2 \cdots x_n$ (det)

(Viète's Formulas, 1579)

"Newton's Theorem".
The evaluation map

$$\varphi_{e_1, \ldots, e_n} : F[x_1, \ldots, x_n] \longrightarrow \underbrace{F[x_1, \ldots, x_n]^{S_n}}_{\text{symm. polys.}}$$
$$x_i \longmapsto e_i$$

is an <u>isomorphism</u>. Neither injective nor surjective is obvious

Gauss' Proof:

Order the terms lexicographically, i.e. say

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} < x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

if $\exists\, l$ with $\alpha_i = \beta_i$ for $1 \le i < l$ and $\alpha_l < \beta_l$

Surjective?

Consider $f \in F[x_1, \ldots, x_n]^{S_n}$ with leading term $c x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.

Claim: $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$.

☆ Otherwise we have $\alpha_k < \alpha_{k+1}$ for some $k$.

By symmetry $x_k \leftrightarrow x_{k+1}$ we see

$$c\, x_1^{\alpha_1} \cdots x_k^{\alpha_{k+1}} x_{k+1}^{\alpha_k} \cdots x_n^{\alpha_n}$$

is also a term of $f$ with lex-higher degree sequence. Contradiction. ///

Now note $c\, e_1^{\alpha_1-\alpha_2} e_2^{\alpha_2-\alpha_3} \cdots e_{n-1}^{\alpha_{n-1}-\alpha_n} e_n^{\alpha_n} \in R^{S_n}$ has the same leading term as $f$.

Hence $f - c\, e_1^{\alpha_1-\alpha_2} \cdots e_n^{\alpha_n}$ is symm. with smaller leading term. By induction

$$f - c\, e_1^{\alpha_1-\alpha_2} \cdots e_n^{\alpha_n} \in F[e_1, \ldots, e_n]$$

$$\Longrightarrow f \in F[e_1, \ldots, e_n]$$

///

Injective? Proof omitted. $\blacksquare$

Example:

Given $f(x,y) \in F[x,y]$ such that $f(x,y) = f(y,x)$, we can write.

$$f(x,y) = \sum c_{\alpha_1,\alpha_2} (x+y)^{\alpha_1} (xy)^{\alpha_2}$$

for some unique numbers $c_{\alpha_1,\alpha_2} \in F$.

e.g.

$$x^4 + y^4 = (x+y)^4 - 4(x+y)^2(xy) + 2(xy)^2$$

Q: What has this to do with Galois Theory?

A: Goal: Express the roots of $f(x) \in F[x]$ in terms of the coefficients. (i.e. "solve $f$")
By Newton's Theorem, it's enough to express the roots in terms of symm. combinations of the roots.

Translation: let $K$ be split. field of $f(x) \in F[x]$. Then $\forall \mu \in Gal(K/F)$, $\alpha \in K$,

$$\mu(f(\alpha)) = f(\mu(\alpha)). \quad \text{Hence}$$

$$f(\alpha) = 0 \iff \mu(f(\alpha)) = 0 \iff f(\mu(\alpha)) = 0$$

i.e. $\mu$ permutes the roots of $f$.

Suppose $f$ has roots $r_1, r_2, \ldots, r_n$,
so $K = F(r_1, r_2, \ldots, r_n)$.

We get a group homomorphism

$$Gal(K/F) \longrightarrow S_n = S_{\{r_1, \ldots, r_n\}}$$

It's <u>injective</u> because if $\mu(r_i) = r_i \ \forall i$
then $\mu(\alpha) = \alpha \ \forall \alpha \in K$.
(the $r_i$ generate $K/F$).
Hence $\mu = id \in Gal(K/F)$.

Hence $Gal(K/F) \leq S_n$.

Furthermore, every $a \in K$ is a poly. in $r_1, r_2, \ldots, r_n$.

<u>Proof</u>: Let

$$\begin{array}{ccccccccc} F & \subseteq & F(r_1) & \subseteq & F(r_1, r_2) & \subseteq \cdots \subseteq & F(r_1, \ldots, r_{n-1}) & \subseteq & K \\ \| & & \| & & \| & & \| & & \| \\ F_0 & \subseteq & F_1 & \subseteq & F_2 & \subseteq \cdots \subseteq & F_{n-1} & \subseteq & F_n \end{array}$$

By induction suppose every elt. of $F_i$ is a poly. in $r_1, \ldots, r_i$ with coeffs. $\in F$. Then $F_{i+1} = F_i(r_{i+1}) \supseteq F_i$ is a simple alg. extension

$\Longrightarrow$ $\forall\, \alpha \in F_{i+1}$ we have

$$\alpha = \sum_k a_k (r_{i+1})^k \quad \text{with } a_k \in F_i$$
$$= \text{poly in } r_1, \ldots, r_{i+1} \ / F.$$

$\boxtimes$

So given $\alpha \in K = F(r_1, \ldots, r_n)$ we can write $\alpha = p(r_1, r_2, \ldots, r_n)$ for some poly $p(\bar{x}) \in F[x_1, \ldots, x_n]$

"$p$ is symmetric"

$\Longleftrightarrow$ $\mu p = p \quad \forall\, \mu \in S_n.$ $\overset{\sim}{\Longleftrightarrow}$ $\mu(\alpha) = \alpha$
$\forall\, \mu \in Gal(K/F)$