2C Automorphisms and fixed fields

The main idea of Galois was to associate to every polynomial $f \in k[X]$ a group of permutations of the zeros of f

In this section we define and study this group and give some numerical information about it.

The description given here is not the originally given by Galois, but an equivalent description given by E. Artin

2.C.1 Galois group of a field extension. Let K be a field. Then the set

$$\mathrm{Aut}\, K = \{\sigma : K \longrightarrow K \mid \sigma \text{ is an automorphism of fields}\}$$

of K forms a group under the operation of composition of maps (in general this group is not abelian).

It was Galois' remarkable discovery that many questions about fields (especially about the zeros of polynomials over a field K) are infact equivalent to certain group theoretical questions in the automorphism group $\mathrm{Aut}\, K$ of the field K; moreover, these questions usually involve not only K, but also subfields of K. Therefore we deal with field extensions $K|k$. Since the k-module (k-vector space) structure of K is of much significance it seems natural to consider:

$$G(K|k) = \mathrm{Gal}(K|k) = \mathrm{Aut}_{k\text{-alg}}\, K = \{\sigma \in \mathrm{Aut}\, K \mid \sigma \text{ is } k\text{-linear} \Leftrightarrow \sigma(a) = a \ \forall a \in k, \text{ i.e. } \sigma|k = \mathrm{id}_k\}$$

It is clear that $G(K|k)$ is a subgroup of the automorphism group $\mathrm{Aut}_{k\text{-alg}} K$ of K. This group is called the <u>Galois group of K over k</u>. Elements of $G(K|k)$ are called k-<u>automorphisms</u> of K or <u>automorphisms of K over k</u>. Further, every k-endomorphism (k-linear and ring homomorphism, i.e. <u>k-algebra homomorphism</u>) $K \longrightarrow K$ is injective (since K is a field) and hence bijective if $K|k$ is finite, i.e. if $[K:k]<\infty$.

If K is generated over k by a subset $\underline{x} \subseteq K$, i.e. $K = k(\underline{x})$, then k-automorphisms of K are uniquely determined by their action on the generating set $\underline{x}$. For example, if $K = k(x_1, \cdots, x_n)$ is generated by the zeros $x_1, \cdots, x_n$ of the polynomial $f \in k[X]$ over k, then the following two lemmas will allow us to interpret the Galois group $\mathrm{Gal}(K|k)$ as a group of permutations of the zeros of f, i.e. a subgroup of the permutationgroup $\mathfrak{S}(\{x_1, \cdots, x_n\}) = \mathfrak{S}_n$. One use of these two lemmas is to help to calculate Galois groups

2.C.1 Lemma Let $K = k(\underline{x})$ be a field extension of a field k which is generated over k by a subset $\underline{x}$ of K and let $\sigma, \tau \in \mathrm{Gal}(K|k)$. Then $\sigma = \tau$ if and only if $\sigma|\underline{x} = \tau|\underline{x}$. In particular, k-automorphisms of K are uniquely determined by their values on a generating set of K over k.

<u>Proof</u> Let $y \in K = k(\underline{x})$. Then there is a finite subset $\{x_1, \cdots, x_n\} \subseteq \underline{x}$ such that $y \in k(x_1, \cdots, x_n)$, i.e. $y = \frac{f(x_1, \cdots, x_n)}{g(x_1, \cdots, x_n)}$, $f, g \in k[X_1, \cdots, X_n]$, $g(x_1, \cdots, x_n) \neq 0$. Since σ and τ are k-

linear and respect addition and multiplication in K

We have $\sigma(y) = \sigma\left(f(x_1,\dots,x_n)/g(x_1,\dots,x_n)\right) = \frac{f(\sigma(x_1),\dots,\sigma(x_n))}{g(\sigma(x_1),\dots,\sigma(x_n))}$

$$= \frac{f(\tau(x_1),\dots,\tau(x_n))}{g(\tau(x_1),\dots,\tau(x_n))} = \tau\left(\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}\right) = \tau(y).$$ Therefore

$\sigma = \tau$.

2.C.3 Proposition Let $K|k$, $L|k$ be field extension and let $\sigma : K \longrightarrow L$ be a k-homomorphism ($=k$-algebra homomorphism). Let $x \in K$ be algebraic over k. Then: if x is a zero of $f \in k[X]$, then $\sigma(x)$ is also a zero of f. In particular, σ permutes the zeros of the minimal polynomial μ_x and $\mu_x = \mu_{\sigma(x)}$.

Proof Let $f = a_0 + a_1X + \dots + a_nX^n \in k[X]$ be such that $f(x) = 0$. Then $0 = \sigma(0) = \sigma(f(x)) = f(\sigma(x))$. In particular, $\mu_x(\sigma(x)) = 0$ and hence $\mu_{\sigma(x)}$ divides μ_x in $k[X]$. Therefore $\mu_{\sigma(x)} = \mu_x$, since μ_x is irreducible in $k[X]$.

2.C.4 Corollary Let $K|k$ be a finite field extension. Then $\mathrm{Gal}(K|k)$ is a finite group.

Proof Since $K|k$ is a finite extension, $K = k(x_1,\dots,x_n)$ for some $x_1,\dots,x_n$ which are algebraic over k. Then, since every $\sigma \in \mathrm{Gal}(K|k)$ is uniquely determined by its values $\sigma(x_1),\dots,\sigma(x_n)$ on $x_1,\dots,x_n$ respectively and by 2.C.3 there are only finitely many possibilities for each $\sigma(x_i)$, (namely $\in V_K(\mu_{x_i})$), there are only finitely many k-automorphisms of K, i.e. $\mathrm{Gal}(K|k)$ is finite.

2.C.5 Examples

(1) $\mathrm{Aut}\,\mathbb{Q} = \{id_{\mathbb{Q}}\}$, $\mathrm{Aut}\,\mathbb{Z}_p = \{id_{\mathbb{Z}_p}\}$ and

$\mathrm{Aut}\,\mathbb{R} = \{id_{\mathbb{R}}\}$. In particular, $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \{id_{\mathbb{R}}\}$ is the trivial group (Since every positive element of $\mathbb{R}$ is a square, every automorphism of $\mathbb{R}$ sends to positive elements and hence it preserves the order $\mathbb{R}$) It is interesting to note that $\mathrm{Aut}\,\mathbb{C}$ is infinite, even though $[\mathbb{C} : \mathbb{R}] = 2$.

(2) The Galois group $\mathrm{Gal}(\mathbb{C}|\mathbb{R})$ of $\mathbb{C}$ over $\mathbb{R}$ is $\{id_{\mathbb{C}}, \sigma\}$ where σ is the complex conjugation $z \longmapsto \bar{z}$ ($\sigma^2 = id_{\mathbb{C}}$). In particular, $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) \cong \mathbb{Z}_2$ = the cyclic group of order 2.

(3) Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$ be the real cube root of 3 and $K = \mathbb{Q}(\alpha)$. Then $\mu_{\alpha,\mathbb{Q}} = X^3 - 2$ and the zeros of $\mu_{\alpha,\mathbb{Q}}$ are $\alpha, \zeta_3 \cdot \alpha, \zeta_3^2 \alpha$, where $\zeta_3 = e^{2\pi i/3}$. Therefore α is the only zero of $\mu_{\alpha,\mathbb{Q}}$ in $\mathbb{Q}(\alpha)$ (for instance, if $\zeta_3 \alpha \in K$, then $\zeta_3 = (\zeta_3 \alpha)\alpha^{-1} \in K$, but $K \subseteq \mathbb{R}$ and $\zeta_3 \notin \mathbb{R}$) If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then $\sigma(\alpha) = \alpha$. This proves that $\sigma = id_K$ and hence $\mathrm{Gal}(K/\mathbb{Q})$ is the trivial group $\{id_K\}$

(4) Let $K = \mathbb{F}_2(t)$ be the rational function in one indeterminate t over $\mathbb{F}_2$ and let $L = \mathbb{F}_2(t^2)$. Then $[L : \mathbb{F}_2] = 2$ and $\mu_t = X^2 - t^2 = (X - t)^2$ in $K[X]$ and hence t is the only zero of $\mu_{t,L}$ in K. Consequen[tly] if $\sigma \in \mathrm{Gal}(K|L)$, then $\sigma(t) = t$ and so $\sigma = id_K$. This proves that $\mathrm{Gal}(K/L) = \{id_K\}$.

(5) Let $p = 1+X+X^2 \in \mathbb{F}_2[X]$. Then p is the only irreducible quadratic polynomial in $\mathbb{F}_2[X]$. Let $K = \mathbb{F}_2[X]/(p(X)) = \mathbb{F}_2[x] = \mathbb{F}_2(x)$. Then $[K:\mathbb{F}_2]=2$, $\mu_{x,\mathbb{F}_2} = p = 1+X+X^2$ and $\mu_{x,\mathbb{F}_2} = (X-x)(X-x-1)$ in $K[X]$. Therefore if $\sigma \in \mathrm{Gal}(K|\mathbb{F}_2)$, then either $\sigma(x)=x$ or $\sigma(x) = x+1$ and hence the group $\mathrm{Gal}(K|\mathbb{F}_2)$ has at most two elements. To see that $\mathrm{Gal}(K|\mathbb{F}_2)$ has exactly two elements, we need to check that the map $\sigma : K \longrightarrow K$ defined by $\sigma(a+bx) \longmapsto a+b(x+1)$ is an $\mathbb{F}_2$-automorphism of K. For this it is enough (since $\{1,x\}$ is a $\mathbb{F}_2$-basis of K) to check that $\sigma(x^2) = \sigma(x)^2$, this equality is immediate from the equality $x^2 = x+1$ in K. This proves that $\mathrm{Gal}(K|\mathbb{F}_2) = \{id_K, \sigma\}$ (Note that $\sigma^2(x) = \sigma(\sigma(x)) = \sigma(x+1) = \sigma(x)+1 = x+1+1 = x$, i.e $\sigma^2 = id_K$).

(6) Let k be a field and $K = k(X)$ be a rational function field in X over k. For each $a \in k$, $0 \neq a$, the map $\sigma_a : K \longrightarrow K$ defined by $\sigma_a(f/g) = f(aX)/g(aX)$ is a k-automorphism of K. Further, for $a, a' \in k^\times$, we have $\sigma_a = \sigma_{a'} \iff a = a'$. Similarly, for each $b \in k$, the map $\tau_b : K \longrightarrow K$ defined by $\tau_b(f/g) = \dfrac{f(X+a)}{g(X+a)}$ is a k-automorphism of K. Further, for $b, b' \in k$, $\tau_b = \tau_{b'} \iff b = b'$. Moreover, if $a \neq 1$ and $b \neq 0$, then $\sigma_a \tau_b \neq \tau_b \sigma_a$ (since $a(X+b) = \sigma_a\tau_b(X) \neq \tau_b\sigma_a(X) = aX+b$. Therefore $\mathrm{Gal}(K/k)$ is non-abelian and if k is infinite then it is infinite.

For each field extension K/k, we have associated a group $\mathrm{Gal}(K/k)$. Moreover, if K/k is finite, then the group $\mathrm{Gal}(K/k)$ is finite. The main idea of Galois theory is to be able to go back and forth from field extensions to groups.

More generally, if L is a field with $k \subseteq L \subseteq K$, then we can associate a group $\mathrm{Gal}(K/L)$ which is a subgrou of $\mathrm{Gal}(K/k)$ (see 2.C.7). Conversely, given a subgroup of $\mathrm{Gal}(K/k)$ we can associate a subfield of K containing k. We shall do this for any subset Σ of $\mathrm{Aut}\,K$

2.C.6 Definition Let K be any field and let $\Sigma \subseteq \mathrm{Aut}\,K$. Let

$$\mathrm{Inv}_K(\Sigma) = I_K(\Sigma) = K^{\Sigma} := \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in \Sigma\}.$$

It is clear that $I_K(\Sigma)$ is a subfield of K, called the fixed field of Σ or field of Σ-invariants of K.

If K/k is a field extension and if $\Sigma \subseteq \mathrm{Gal}(K/k)$, then $k \subseteq I_K(\Sigma) \subseteq K$, i.e. $I_K(\Sigma)$ is an intermediate field of the extension K/k.

In the following lemma we list simple properties of Galois groups and fixed fields:

2.C.7 Lemma Let K be a field

(1) If $L_1 \subseteq L_2$ are subfields of K, then $\mathrm{Gal}(K/L_2) \subseteq \mathrm{Gal}(K/L_1)$

(2) If L is a subfield of K, then $L \subseteq \mathrm{Inv}_K(\mathrm{Gal}(K/L))$

(3) If $\Sigma_1 \subseteq \Sigma_2 \subseteq \mathrm{Aut}\,K$ are subsets (of $\mathrm{Aut}\,K$), then

$\mathrm{Inv}_K(\Sigma_2) \subseteq \mathrm{Inv}_K(\Sigma_1)$.

(4) If $\Sigma \subseteq \mathrm{Aut}\,K$ is a subset of $\mathrm{Aut}\,K$, then $\Sigma \subseteq \mathrm{Gal}(K/\mathrm{Inv}_K(\Sigma))$.

(5) If $L = \mathrm{Inv}_K(\Sigma)$ for some subset $\Sigma \subseteq \mathrm{Aut}\,K$, the $L = \mathrm{Inv}_K(\mathrm{Gal}(K/L))$.

(6) If $H = \mathrm{Gal}(K/L)$ for some subfield L of K, then $H = \mathrm{Gal}(K/\mathrm{Inv}_K(H))$.

Proof (1) If $\sigma \in \mathrm{Gal}(K/L_2)$, then $\sigma(a) = a \quad a \in L_2$ and hence $\sigma(a) = a$ for all $a \in L_1$, since $L_1 \subseteq L_2$. Therefor $\sigma \in \mathrm{Gal}(K/L_1)$.

(2), (3) and (4) are simple consequences of definitions.

(5) Suppose that $L = \mathrm{Inv}_K(\Sigma)$ for some $\Sigma \subseteq \mathrm{Aut}\,K$. Then $\Sigma \subseteq \mathrm{Gal}(K/L)$ and so $\mathrm{Inv}_K(\mathrm{Gal}(K/L)) \underset{(3)}{\subseteq} \mathrm{Inv}_K(\Sigma)$ $L \underset{(2)}{\subseteq} \mathrm{Inv}_K(\mathrm{Gal}(K/L))$. This proves that $L = \mathrm{Inv}_K(\mathrm{Gal}(K/L))$

(6) Suppose that $H = \mathrm{Gal}(K/L)$ for some subfield of K. Then $L \subseteq \mathrm{Inv}_K(\mathrm{Gal}(K/L)) = \mathrm{Inv}_K(H)$ and so $\mathrm{Gal}(K/\mathrm{Inv}_K(H))$ $\underset{(1)}{\subseteq} \mathrm{Gal}(K/L) = H \underset{(4)}{\subseteq} \mathrm{Gal}(K/\mathrm{Inv}_K(H))$. Therefore $H = \mathrm{Gal}(K/\mathrm{Inv}_K(H))$.

2.C.8 Corollary Let K be a field. Then the maps

$$\{\text{Subfields of } K\} \xrightarrow{G_K := \mathrm{Gal}(K|-)} \{\text{Subgroups of } \mathrm{Aut}\,K\},$$
$$L \longmapsto \mathrm{Gal}(K|L)$$

and

$$\{\text{Subgroups of } \operatorname{Aut} K\} \xrightarrow{I_K := \operatorname{Inv}_K(-)} \{\text{Subfields of } K\},$$
$$H \longmapsto \operatorname{Inv}_K(H)$$

are inclusion reversing. Moreover,

$$I_K \circ G_K \circ I_K = I_K \quad \text{and} \quad G_K \circ I_K \circ G_K = G_K .$$

In particular, the maps $\operatorname{Im}(I_K) \xrightarrow{G_K} \operatorname{Im}(G_K)$ and $\operatorname{Im}(G_K) \xrightarrow{I_K} \operatorname{Im}(I_K)$ are inclusion reversing inverses of each other.

Proof Immediate from 2.c.7 (5)-(6).

2.c.9 Corollary Let $K|k$ be a field extension. Then the maps

$$\mathcal{F}(K|k) := \left\{\begin{matrix}\text{Subfields of } K \\ \text{containing } k\end{matrix}\right\} \xrightarrow{G_{K|k}} \left\{\begin{matrix}\text{Subgroups of} \\ \operatorname{Gal}(K|k)\end{matrix}\right\} = \mathcal{S}(\operatorname{Gal}(K|k))$$
$$L \longmapsto \operatorname{Gal}(K|L)$$

and

$$\mathcal{S}(\operatorname{Gal}(K|k)) \xrightarrow{I_{K|k}} \mathcal{F}(K|k),$$
$$H \longmapsto \operatorname{Inv}_K(H)$$

are inclusion reversing. Moreover,

$$I_{K|k} \circ G_{K|k} \circ I_{K|k} = I_{K|k} \quad \text{and} \quad G_{K|k} \circ I_{K|k} \circ G_{K|k} = G_{K|k}$$

In particular, the maps $\operatorname{Im}(I_{K|k}) \xrightarrow{G_{K|k}} \operatorname{Im}(G_{K|k})$ and $\operatorname{Im}(G_{K|k}) \xrightarrow{I_{K|k}} \operatorname{Im}(I_{K|k})$ are inclusion reversing inverses of each other.

Now, suppose that $K|k$ is a finite extension. Our main interest is to find conditions such that the maps $I_{K|k}$ and $G_{K|k}$ are bijective. First note tha $I_{K|k}$ is bijective if and only if $G_{K|k}$ is bijective (use 2.C.9). Moreover, from 2.C.7-(5) it follows that a necessary condition for $I_{K|k}$ to be surjective is that $k \in \mathrm{Im}(I_{K|k})$, i.e. $k = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$.

We shall see in the next three sections that this condition is actually a sufficient condition. This will be established by forging the link between the present "abstract" Galois theory and the theory of equations.

Further in this section we aim to get more precise numerical information on $|\mathrm{Gal}(K|k)|$ for a finite field extension. More precisely, we prove:

2.C.10 Theorem Let K be a field

(1) ~~If~~ $K|k$ is a finite field extension, then

$$|\mathrm{Gal}(K|k)| \leq [K:k].$$

(2) Let $G \subseteq \mathrm{Aut}\, K$ be a finite group of automorphisms of K with $k = \mathrm{Inv}_K(G)$. Then:

$$|G| = [K:k]. \text{ In particular, } G = \mathrm{Gal}(K|k).$$

For the proof of this theorem we need the following Dedekind's lemma on the independence of characters on a group with values in a field. First let us recall:

2.C.11 Definition Let G be a group and let K be a field. A character on G with values in K is a group homomorphism from G to $K^\times$ (= the multiplicati group of K).

For example, every automorphism of the field K is a character on $K^\times$ with values in K. In particular, every element of $\mathrm{Gal}(K/k)$ is a character on $K^\times$ with values in K.

2.C.12 Lemma (Dedekind) Let G be a group and let K be a field. Let $\sigma_1, \cdots, \sigma_n$ be distinct characters on G with values in K. Then $\sigma_1, \cdots, \sigma_n$ are linearly independen over K, i.e. if $\left(\sum a_i \sigma_i\right)(g) = 0$ for all $g \in G$, where $a_1, \cdots, a_n \in K$, then $a_1 = \cdots = a_n = 0$.

Proof Suppose that (if necessary renumber $\tau_1, \cdots, \tau_n$) r is the least integer $1 \le r \le n$ with

$$a_1\tau_1 + \cdots + a_r\tau_r = 0 \quad \text{with } a_1, \cdots, a_r \in K.$$

Then all $a_1, \cdots, a_r$ are non-zero and

$$a_1\tau_1(g) + \cdots + a_r\tau_r(g) = 0 \quad \text{for all } g \in G.$$

Since $\tau_1 \neq \tau_2$, $\tau_1(h) \neq \tau_2(h)$ for some $h \in G$. Further,

(1) $\quad a_1\tau_1(h)\tau_1(g) + a_2\tau_1(h)\tau_2(g) + \cdots + a_r\tau_1(h)\cdot\tau_r(g) = 0$ for all $g \in$

and

$a_1\tau_1(hg) + a_2\tau_2(hg) + \cdots + a_r\tau_r(hg) = 0$ for all $g \in$

(2) $\quad a_1\tau_1(h)\tau_1(g) + a_2\tau_2(h)\tau_2(g) + \cdots + a_r\tau_r(h)\tau_r(g) = 0$ for all $g \in$

Now, substracting (2) from (1), we get:

$$a_2\left(\tau_1(h) - \tau_2(h)\right)\tau_2(g) + \cdots + a_r\left(\tau_1(h) - \tau_r(h)\right)\tau_r(g) = 0 \text{ for all } g \in$$

i.e. $\quad a_2\left(\tau_1(h) - \tau_2(h)\right)\tau_2 + \cdots + a_r\left(\tau_1(h) - \tau_r(h)\right)\tau_r = 0$, this contradicts the minimality of r, since $a_r\left(\tau_1(h) - \tau_2(h)\right) \neq 0$ by the choice of h.

2.C.13 Remark. Let K be a field and G be a group. Then K^G is a K-vector space (with componentwise addition and scalar multiplication) and $\mathrm{Hom}_{\text{groups}}(G, K^*) \subseteq K^G$.

Then the subset $\mathrm{Hom}_{\text{groups}}(G, K^*)$ of K^G is linearly independent (immediate from 2.C.12).

Now, we come to the proof of the theorem 2.C.10.

Proof of 2.C.10:

(1) The group $\mathrm{Gal}(K|k)$ is finite by 2.C.4. Let $\mathrm{Gal}(K|k) = \{\tau_1, \cdots, \tau_n\}$. Suppose on contrary $m = [K : k] \lneq |\mathrm{Gal}(K|k)|$. Let $x_1, \cdots, x_m \in K$ be a k-basis of K. Then the $n \times m$ matrix

$$\mathfrak{A} = (\tau_i(x_j))_{\substack{1 \le i \le n \\ 1 \le j \le m}} = \begin{pmatrix} \tau_1(x_1) & \tau_1(x_2) & \cdots & \tau_1(x_m) \\ \tau_2(x_1) & \tau_2(x_2) & \cdots & \tau_2(x_m) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(x_1) & \tau_n(x_2) & \cdots & \tau_n(x_m) \end{pmatrix} \in$$

$M_{n,m}(K)$ has rank $\le \mathrm{Min}(n,m) = m < n$ and hence the rows of $\mathfrak{A}$ are linearly dependent over K, i.e. there exist $a_1, \cdots, a_n \in K$, not all zero, such that

$$a_1\tau_1(x_j) + a_2\tau_2(x_j) + \cdots + a_n\tau_n(x_j) = 0 \text{ for all } j = 1, \cdots, m.$$

Therefore $a_1\tau_1(x) + a_2\tau_2(x) + \cdots + a_n\tau_n(x) = 0$ for all $x \in K$, since $x_1, \cdots, x_m$ is a k-basis of K and $\tau_1, \cdots, \tau_n$ are k-linear. In particular, $a_1\tau_1 + \cdots + a_r\tau_r = 0$ with not all $a_1, \cdots, a_n$ are zero, i.e. the characters $\tau_1, \cdots, \tau_n$ on K^* with values in K are linearly dependent over K, a contradiction to Dedekind's lemma 2.C.12.

(2) Since $G \subseteq Gal(K/k)$, $|G| \leq |Gal(K/k)| \leq [K:k]$ by part (1). Suppose that $n := |G| < [K:k]$. Then $G = \{\tau_1, \cdots, \tau_n\}$ and choose $x_1, \cdots, x_{n+1} \in K$ which are linearly independent over k. The matrix

$$\mathfrak{A} = (\tau_i(x_j))_{\substack{1\leq i\leq n \\ 1\leq j\leq n+1}} = \begin{pmatrix} \tau_1(x_1) & \tau_1(x_2) & \cdots & \tau_1(x_{n+1}) \\ \tau_2(x_1) & \tau_2(x_2) & \cdots & \tau_2(x_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(x_1) & \tau_n(x_2) & \cdots & \tau_n(x_{n+1}) \end{pmatrix}$$

$\in M_{n,n+1}(K)$ has rank $\leq \mathrm{Min}(n, n+1) = n$ and hence the columns of $\mathfrak{A}$ are linearly dependent over K. Now, (if necessary renumber $x_1, \cdots, x_{n+1}$) the least integer with $1 \leq r \leq n+1$ and choose $a_1, \cdots, a_r \in K$ such that

$$a_1 \begin{pmatrix} \tau_1(x_1) \\ \vdots \\ \tau_n(x_1) \end{pmatrix} + a_2 \begin{pmatrix} \tau_1(x_2) \\ \vdots \\ \tau_n(x_2) \end{pmatrix} + \cdots + a_r \begin{pmatrix} \tau_1(x_r) \\ \vdots \\ \tau_n(x_r) \end{pmatrix} = 0.$$

Then all $a_1, \cdots, a_r$ are non-zero by minimality of r and hence we may assume $a_1 = 1$. Therefore

(a). $\sum_{i=1}^{r} a_i \tau_j(x_i) = 0$ for all $j = 1, \cdots, n$, i.e.

$\tau_j\left(\sum_{i=1}^{r} a_i x_i\right) = 0$ for all $j = 1, \cdots, n$ and hence

(c) $\sum_{i=1}^{r} a_i x_i = 0$, since τ_j is injective. Now, for each $\sigma \in G$, we hav

(b) $0 = \sigma\left(\sum_{i=1}^{r} a_i \tau_j(x_i)\right) = \sum_{i=1}^{r} \sigma(a_i) \tau_j(x_i)$ for all $j = 1, \cdots, n$,

since σ permutes $\tau_1, \cdots, \tau_n$, i.e. $\{\sigma\tau_1, \cdots, \sigma\tau_n\} = \{\tau_1, \cdots, \tau_n\}$

Therefore, since $a_1 = 1$, substracting (b) from (a) we get:

$$\sum_{i=2}^{r} \left(a_i - \sigma(a_i)\right) \tau_j(x_i) = 0 \quad \text{for all } j = 1, \cdots, n$$

and hence $a_i = \sigma(a_i)$ for all $i = 2, \cdots, r$, by minimality of r. Since this is true for all $\sigma \in G$, we get all $a_1, a_2, \cdots, a_r \in \mathrm{Inv}_K(G) = k$. But now from the equation (c), we get all $a_1 = \cdots = a_r = 0$, since $x_1, \cdots, x_n$ are linearly independent over k, which is absurd, since $a_1 = 1$.

The field extensions described in 2.C.10 (2) are of particular interest, since they were used by Galois to study the solvability of polynomials.

2.C.14 Definition Let $K|k$ be an algebraic field extension. We say that K is <u>Galois</u> over k if $k = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$.

Note that if $K|k$ is a finite field extension, then 2.C.10 (2) give a numerical criterion for when K is Galois over k

2.C.15 Corollary Let $K|k$ be a finite field extension. Then $K|k$ is Galois if and only if $|\mathrm{Gal}(K|k)| = [K:k]$

Proof ($\Rightarrow$) If $K|k$ is Galois, then $k = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$ and so $|\mathrm{Gal}(K|k)| = [K:k]$ by 2.C.10-(2).

($\Leftarrow$) If $|\mathrm{Gal}(K|k)| = [K:k]$ and $L = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$. Then $\mathrm{Gal}(K|L) = \mathrm{Gal}(K|k)$ by 2.C.10-(2) and so.

Therefore, since $a_1 = 1$, substracting (b) from (a) we get:

$$\sum_{i=2}^{r} \left(a_i - \sigma(a_i)\right) \tau_j(x_i) = 0 \quad \text{for all } j = 1, \cdots, n$$

and hence $a_i = \sigma(a_i)$ for all $i = 2, \cdots, r$, by minimality of r. Since this is true for all $\sigma \in G$, we get all $a_1, a_2, \cdots, a_r \in \mathrm{Inv}_K(G) = k$. But now from the equation (c), we get all $a_1 = \cdots = a_r = 0$, since $x_1, \cdots, x_n$ are linearly independent over k, which is absurd, since $a_1 = 1$.

The field extensions described in 2.C.10 (2) are of particular interest, since they were used by Galois to study the solvability of polynomials.

<u>2.C.14 Definition</u> Let $K|k$ be an algebraic field extension. We say that K is <u>Galois</u> over k if $k = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$.

Note that if $K|k$ is a finite field extension, then 2.C.10 (2) give a numerical criterion for when K is Galois over k

<u>2.C.15 Corollary</u> Let $K|k$ be a finite field extension. Then $K|k$ is Galois if and only if $|\mathrm{Gal}(K|k)| = [K:k]$

<u>Proof</u> ($\Rightarrow$) If $K|k$ is Galois, then $k = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$ an so $|\mathrm{Gal}(K|k)| = [K:k]$ by 2.C.10-(2).
($\Leftarrow$) If $|\mathrm{Gal}(K|k)| = [K:k]$ and $L = \mathrm{Inv}_K(\mathrm{Gal}(K|k))$. The $\mathrm{Gal}(K|L) = \mathrm{Gal}(K|k)$ by 2.C.10-(2) and so.