From (i) it follows that we can reorder $1, 2, \dots, n+1$ giving $i_1, \dots, i_{n+1}$ so that for each k, $\sigma\tau_k$ and τ_{i_k} are in the same coset of H in J.

Then from (ii), since $\sigma\tau_k(u_i) = \tau_{i_k}(u_i)$ the k^{th} equation of $(*)$ is actually the $i_k{}^{th}$ equation of our original system

When the groups H, J are closed or the fields L, M are closed, everything is easier:

Lemma 2.10: Let $K \subset L \subset M \subset F$ be fields and $\{id\} < H < J < \mathrm{Aut}_K F$ groups. Then.

(i) If L is closed and $[M:L] < \infty$ then $|L':M'| = [M:L]$
and M is closed.

(ii) If H is closed and $|J:H| < \infty$ then $[H':J'] = |J:H|$.
and J is closed.

(iii) If $[F:K] < \infty$ and F is a Galois extension of K, then all intermediate fields and subgroups are closed, and $|\mathrm{Aut}_K F| = [F:K]$.

Proof: First we prove (ii):

$$|J:H| \le |J'':H| = |J'':H''| \le [H':J'] \le |J:H|$$

since $J < J''$

H is closed

~~since $J''' = J'$ and $H''' = H'$,~~

Then apply Lemma 2.8

Apply Lemma 2.9.

But this means $|J'' : H| = |J : H|$, and since $J < J''$ this gives $J = J''$. It also gives $[H' : J'] = |J : H|$.

The proof of (i) is nearly identical.

To prove (iii), suppose $K \leq E \leq F$, then $[F : K] < \infty \Rightarrow [E : K] < \infty$. Since F is Galois over K, we have $K = K''$, and so (i) implies that $|K' : E'| = [E : K]$ and E is closed. In particular if $E = F$ then $|\mathrm{Aut}_K F| = [F : K]$.

On the other hand if $J < \mathrm{Aut}_K F$, then $\{id\}$ is closed ($\{id\}' = F$, $F' = \{id\}$) and so a similar argument using (ii) shows J is closed.

Withe these lemmas, part (a) of the fundamental theorem is easy. To do part (b), we must determine which fields correspond to normal subgroups.

<u>Definition</u>: If $K \subseteq F$ are fields and E is an intermediate field, then E is called <u>stable</u> if $\sigma(e) \in E$ for all $e \in E$ and all $\sigma \in \mathrm{Aut}_K F$.

<u>Remark</u>:
- This implies that the restriction $\sigma|_E$ is an element of $\mathrm{Aut}_K E$
- It turns out that $[F:K] < \infty \Rightarrow E$ stable $\Leftrightarrow E/K$ Galois.

<u>Lemma 2.11</u>: Let F be an extension of K.

(i) If $K \subseteq E \subseteq F$ and E is stable, then
$$E' = \mathrm{Aut}_E F \triangleleft \mathrm{Aut}_K F \quad \text{(normal)}$$

(ii) If $H \triangleleft \mathrm{Aut}_K F$ then H' is stable

<u>Proof</u>: Let us prove (i) first.

If $u \in E$ and $\sigma \in \mathrm{Aut}_K F$, and $\tau \in \mathrm{Aut}_E F$, then since $\sigma(u) \in E$ by stability we have $\tau\sigma(u) = \sigma(u)$. Thus $\sigma^{-1}\tau\sigma^{-1}(u) = u$ for all $e \in E$, thus $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_E F$ and so $\mathrm{Aut}_E F$ is normal.

(ii) Same reasoning, in reverse. Suppose $\tau \in H$ and $\sigma \in \mathrm{Aut}_K F$. Then $\sigma^{-1}\tau\sigma \in H$ so $\sigma^{-1}\tau\sigma(a) = u$ for all $u \in H'$

$\Rightarrow \tau\sigma(u) = \sigma(u)$ for all $u \in H'$ and all $\tau \in H$.

But then $\sigma(u) \in H'$, meaning H' is stable.

How is stability related to Galois extensions?

<u>Lemma: 2.12</u>: If F is a Galois extension of K and E is a stable intermediate field, then E is Galois over K.

<u>Proof</u>: If $u \in E \setminus K$, then there's $\sigma \in \mathrm{Aut}_K F$ with $\sigma(u) \neq u$ since F is Galois over K. By stability, $\sigma(u) \in E$, thus $\sigma|_E$ is an element of $\mathrm{Aut}_K E$ which moves u. Thus $(\mathrm{Aut}_K E)' = K$, so E/K is Galois.

<u>Lemma 2.13</u>: If $K \subseteq E \subseteq F$ and E is algebraic and Galois over K, then E is stable.

<u>Proof</u>: If $u \in E$, let $f(x) \in K[x]$ be its minimal polynomial. Let $u_1, \ldots, u_r$ be the roots of f that are in E, note $r \leq n = \deg f$.

Now if $\tau \in \mathrm{Aut}_K E$, τ permutes the roots of f that are in E. Thus the corresponding automorphism of $E[x]$ must fix the polynomial $(x-u_1)(x-u_2)\cdots(x-u_r) = g(x)$, meaning τ fixes the coefficients of this polynomial. But since this holds for every $\tau \in \mathrm{Aut}_K E$ and E is Galois over K, this implies $g(x) \in K[x]$.

But now $f(x), g(x) \in K[x]$ have common roots, and f is irreducible. Thus f divides g, but g is monic and $\deg g \leq \deg f$ so this forces $f = g$. Consequently $u_1, \dots, u_r$ are exactly the roots of f, meaning all roots of f are distinct and lie in E. But now recall: u is an arbitrary element of E, and f its minimal polynomial. Since any $\sigma \in \mathrm{Aut}_K F$ permutes the roots of f, $\sigma(u)$ is another root of f — and thus lies in E. So E is stable.

Remark: Exercise 13 shows that this lemma does not hold if E is not algebraic over K.

As a final ingredient, we need to discuss the quotient $\mathrm{Aut}_K F / \mathrm{Aut}_E F$ when $\mathrm{Aut}_E F$ is normal. In general, we need the following definition to state our result!

Definition: Suppose $K \subseteq E \subseteq F$ fields. We call $\tau \in \mathrm{Aut}_K E$ extendible if $\exists\, \sigma \in \mathrm{Aut}_K F$ such that $\tau = \sigma|_E$.

Lemma 2.14 : Suppose $K \le E \le F$, and E is stable. Then $\mathrm{Aut}_K F / \mathrm{Aut}_E F$ is isomorphic to the group of K-automorphisms of E extendible to F.

Proof: Define a homomorphism $\mathrm{Aut}_K F \longrightarrow \mathrm{Aut}_K E$ by $\sigma \longmapsto \sigma|_E$. The image is clearly all extendible automorphisms, the kernel is $\mathrm{Aut}_E F$. The result follows from the first isomorphism theorem.

Proof of the fundamental theorem of Galois theory :

We saw already that there's a correspondence between closed intermediate fields and closed subgroups. But Lemma 2.10 (iii) shows that for Galois extensions, all subgroups and all intermediate fields are closed. Then (i) follows from Lemma 2.10 (i).

To prove (ii): Suppose $K \le E \le F$. Then F is Galois over E since E is closed ($E = E''$). Assuming $[F:K] < \infty$ (which we do), E is algebraic over K so ~~it~~ if it's Galois over K then it's stable by Lemma 2.13. Then $E' = \mathrm{Aut}_E F$ is normal in $\mathrm{Aut}_K F$ by Lemma 2.11 (i).

On the other hand, if $E' = \mathrm{Aut}_E F$ is normal in $\mathrm{Aut}_K F$, then E'' is stable by Lemma 2.11 (ii). But $E'' = E$ since F/K is Galois, so E is stable over K and hence E/K is Galois, by Lemma 2.12.

Now when E is Galois over K, $E' = \mathrm{Aut}_E F$ is normal in $\mathrm{Aut}_K F$ so we analyze the quotient. Since E and E' are closed, and $(\mathrm{Aut}_K F)' = K$ we can use Lemma 2.10 to get: (write G for $\mathrm{Aut}_K F$)

$$|G/E'| \underset{\text{definition}}{=} |G : E'| \underset{\text{Lemma 2.10}}{=} [E'' : G'] \underset{\text{Since } E \text{ closed, } F/K \text{ Galois}}{=} [E : K]$$

But Lemma 2.14 shows G/E' is isomorphic to a subgroup of $\mathrm{Aut}_K E$. The only way this subgroup can be of size $[E:K]$ is if G/E' is all of $\mathrm{Aut}_K E$, because $|\mathrm{Aut}_K E| = [E:K]$ by part (i) of the theorem

Hungerford §5.3:

Splitting fields, algebraic closure, normality

Since we have a theorem that paints a wonderful picture when $K \subseteq F$ is a Galois extension, our next Goal is: come up with more Galois extensions!

This means we are either going to construct Galois extensions or show that extensions we are provided are Galois. Recall:

Def: Suppose $f \in K[x]$, $\deg f \geq 1$. Then an extension F of K is called a splitting field for f over K if $f(x)$ splits as a product of linear factors:

$$f = (x-u_1)(x-u_2)\cdots(x-u_n) \text{ with } u_i \in F$$

and $F = K(u_1, \dots, u_n)$.

If S is a set of polynomials in $K[x]$, then F is said to be a splitting field for S over K if every $f \in S$ splits over F and if $F = K(X)$ where $X = \{\text{roots of } f \in S\}$.

Remark: If $|S| < \infty$, say $S = \{f_1, f_2, \dots, f_n\}$, then the splitting field for S is the same as the splitting field for $f = f_1 f_2 \cdots f_n$.

<u>Theorem</u>: If $f \in K[x]$ and $\deg f = n \geq 1$, then there exists a splitting field F for f with
$$[F:K] \leq n!$$

<u>Proof</u>: Induct on $n = \deg f$. If $n=1$ or if f splits over K, then $F = K$.

Otherwise suppose $n > 1$ and f does not split over K. Let g be an irreducible factor of f with $\deg g > 1$. Then ~~if u~~ there's an extension $K(u)$ of K with u a root of g and $[K(u):K] = \deg g > 1$. Then
$$f = (x-u)h(x), \quad h(x) \in K(u)[x]$$
$$\deg h(x) = n-1.$$
By induction, h splits over an extension F of $K(u)$ of degree $(n-1)!$ or less. Then F is actually a splitting field of f and
$$[F:K] = [F:K(u)][K(u):K] \leq (n-1)! \cdot \deg g \leq n!$$

When $|S| = \infty$, there always exists a splitting field for S over K as well. The proof is very involved. We give only relevant definitions and sketches of the ideas:

<u>Definition</u>: A field F is called <u>algebraically closed</u> if it satisfies any of the following

equivalent conditions:

(i) Every nonconstant $f \in F[x]$ has a root in F

(ii) Every nonconstant $f \in F[x]$ splits over F

(iii) Every irreducible $f \in F[x]$ has $\deg f = 1$.

(iv) No proper algebraic extensions of F exist

(v) There exists a subfield $K \subset F$ such that F is algebraic over K and every polynomial in $K[x]$ splits over F.

<u>Sketch</u> of equivalence of these properties:

The equivalence of (i)—(iii) is fairly straightforward. To see that F has no proper algebraic extension if (i)-(iii) hold, suppose otherwise. Say L is an algebraic extension, choose $p(x) \in F[x]$ the minimal poly of some $u \in L \setminus F$. But $p(x)$ is irreducible, by (iii) $\deg p = 1$ and so $u \in F$, a contradiction.

On the other hand if F has no proper algebraic extension then let $p(x) \in F[x]$ be irreducible. Then $F[x]/(p(x))$ is an algebraic extension of F, by assumption we must have $F[x]/(p(x)) = F \Longrightarrow \deg p = 1$.

To see (v), note if (iii) is true then we can take $K = F$ in the statement of (v) to see that (v) holds.

On the other hand, suppose (v) holds. Showing that (i), (ii), (iii) or (iv) holds is rather tricky. We <u>defer the proof</u> to later (possibly an assignment).

Essentially, this is the theorem we want:

<u>Theorem</u>: Suppose $K \subseteq F$ are fields. TFAE:

(i) F is algebraic over K and F is algebraically closed,

(ii) F is a splitting field of all irreducible polynomials in $K[x]$.

<u>Theorem</u>: Every field K has an algebraic closure. Any two algebraic closures of K are isomorphic via a K-isomorphism.

<u>Proof</u>: A fair amount of set-theoretic obstacles in the construction. There is a new, clever proof as of 1993 (newer than Hungerford's book) which avoids some of the set-theoretic gripes.