A direct constructive treatment of the Fundamental Theorem of Galois Theory
DRAFT

Peter Aczel

September 29, 1998

The Fundamental Theorem of Galois Theory

This is the basic structure theorem at the heart of Galois Theory. We start with a classical account of the result and then explain how this needs to be modified to get a constructive result. We will restrict attention to fields of characteristic 0.

Let E be a field (of characteristic 0). We write Aut_E for the group of automorphisms of E. The fundamental theorem concerns correspondences each way between the subfields of E and the subgroups of Aut_E. To each subfield F of E is associated the subgroup $F^{\triangle}$ of Aut_E given by

$$F^{\triangle} = \{g \in Aut_E \mid \forall x \in F\ g(x) = x\}.$$

When we want to make explicit the dependence of $F^{\triangle}$ on E we will write it $Gal(E : F)$ and call it the **Galois group of** $E : F$. To each subgroup G of Aut_E is associated the subfield G^{∇} of E given by

$$G^{\nabla} = \{x \in E \mid \forall g \in G\ g(x) = x\}.$$

These correspondences form a Galois connection; i.e. for each F and each G

$$F \subseteq G^{\nabla} \iff G \subseteq F^{\triangle}.$$

It follows that the correspondences are anti-monotone and that for all F and all G

$$G^{\nabla\triangle\nabla} = G^{\nabla} \text{ and } F^{\triangle\nabla\triangle} = F^{\triangle}.$$

If F is a subfield of E and K is a subfield of F then we will also call the subfield F of E a K**-subfield of** E. Call a subfield F of E a **Galois subfield of** E if $F = G^{\nabla}$ for some finite subgroup G of Aut_E. It will be convenient to state the Fundamental Theorem using some special notation for some posets that are partially ordered by the subset relation.

Definition 0.1 *Let E be a field.*

- *$\mathcal{G}(E)$ is the poset of finite subgroups of Aut_E.*
- *$\mathcal{F}(E)$ is the poset of subfields of E of the form G^{∇} where $G \in \mathcal{G}(E)$.*

Let $K \in \mathcal{F}(E)$.

- $\mathcal{G}(E:K)$ *is the poset of subgroups of* $Gal(E:K)$.
- $\mathcal{F}(E:K)$ *is the poset of* K*-subfields of* E.

Theorem 0.2 (Fundamental Theorem)

1. *The map* $F \mapsto Gal(E:F)$ *gives an anti-isomorphism between the posets* $\mathcal{F}(E)$ *and* $\mathcal{G}(E)$.
2. *If* $K \in \mathcal{F}(E)$ *then* $\mathcal{F}(E:K) \subseteq \mathcal{F}(E)$ *and the above anti-isomorphism restricts to an anti-isomorphism between the posets* $\mathcal{F}(E:K)$ *and* $\mathcal{G}(E:K)$.
3. *If* $K \in \mathcal{F}(E)$ *and* F *is a* $\mathcal{F}(E:K)$ *then*
   (a) $K \in \mathcal{F}(F)$ *if and only if* $Gal(E:F)$ *is a normal subgroup of* $Gal(E:K)$,
   (b) *if* $K \in \mathcal{F}(F)$ *then* $Gal(F:K)$ *is isomorphic to the quotient group* $Gal(E:K)/Gal(E:F)$.

1 The constructive version of the Fundamental Theorem

In this section we wish to state the version of the fundamental theorem that can be constructively proved. In fact we will keep exactly to the formulation in the previous section, but refine the definitions of the posets.

Which constructive notion of field should we use? There are several choices. The following one is what we need. It incorporates that the field has characteristic zero; i.e. the sum $1 + \cdots + 1$ of any one or more copies of 1 is non-zero and is discrete; i.e. equality on it is decidable.

Definition 1.1 *By a field we will mean a commutative ring with 1, that is discrete and has characteristic zero, such that every non-zero element has an inverse.*

We now need to refine the definitions of the posets used in our formulation of the Fundamental Theorem. To do so we first need the following important idea of Galois Theory. If F is a subfield of E then we may view E as a vector space over F. We will write $E:F$ for this vector space and when it is finite dimensional we will write $[E:F]$ for its dimension.

In the following refined definitions of the posets we will also need the specifically constructive notions of a strongly finite subset of a set of functions $A \to B$ and of a decidable subset of a set A. As in classical mathematics a set is finite if it is in one-one correspondence with the set $\{1, \ldots, n\}$ for some natural number n. Functions $g_1, g_2 : A \to B$ are equal if $g_1(x) = g_2(x)$ for all $x \in A$ and **apart** if there is some $x \in A$ such that $g_1(x) \neq g_2(x)$. Note that when B is discrete g_1, g_2 are equal if and only if they are not apart. But we cannot generally assert that if g_1, g_2 are not equal then they are apart. If we can assert this for all $g_1, g_2 \in X$, where X is a finite set of functions $A \to B$ then we call the set X **strongly finite**. Finally a subset X of a set A is a **decidable subset of** A if $a \in X$ or $a \notin X$ for all $a \in A$.

Definition 1.2 *Let* E *be a field.*

- $\mathcal{G}(E)$ *is the poset of strongly finite subgroups of* Aut_E.

- *$\mathcal{F}(E)$ is the poset of subfields of E of the form G^{∇} where $G \in \mathcal{G}(E)$.*

Let $K \in \mathcal{F}(E)$.

- *$\mathcal{G}(E : K)$ is the poset of decidable subgroups of $Gal(E : K)$.*
- *$\mathcal{F}(E : K)$ is the poset of finite dimensional K-subfields of E.*

2 The Proof

The Fundamental Theorem will be an easy consequence of the following four results. In these results we assume that G is a strongly finite subgroup of Aut_E.

Theorem 2.1 *$E : G^{\nabla}$ is finite dimensional and $[E : G^{\nabla}] = |G|$.*

Theorem 2.2 *If U is a decidable subgroup of G then G/U is a finite set, $U^{\nabla} : G^{\nabla}$ is finite dimensional and*

$$[U^{\nabla} : G^{\nabla}] = |G/U|.$$

Theorem 2.3 *$G^{\nabla\triangle} = G$.*

Theorem 2.4 *If F is a finite dimensional G^{∇}-subfield of E then*

1. *$F^{\triangle}$ is a strongly finite decidable subgroup of G and $F^{\triangle\nabla} = F$,*
2. *$G_F = Gal(F : G^{\nabla})$ is strongly finite,*
3. *If H is a strongly finite subgroup of Aut_F and $G^{\nabla} = \{x \in F \mid \forall h \in H\ h(x) = x\}$ then $H = G_F$,*
4. *$G^{\nabla} = \{x \in F \mid \forall g \in G_F\ g(x) = x\}$ if and only if $F^{\triangle}$ is a normal subgroup of G,*
5. *If $F^{\triangle}$ is a normal subgroup of G then the quotient group $G/F^{\triangle}$ is isomorphic to the group G_F.*

We now show how to prove the Fundamental Theorem from these theorems.

For 1 Observe that, by Theorem 2.3, the operation $(\ )^{\triangle}$ maps $\mathcal{F}(E)$ into $\mathcal{G}(E)$ and $(\ )^{\nabla}$ maps $\mathcal{G}(E)$ into $\mathcal{F}(E)$ and the two maps are inverses of each other.

For 2 Let $K \in \mathcal{F}(E)$. Then $K = G^{\nabla}$ for some strongly finite subgroup G of Aut_E. By Theorem 2.3 $G = K^{\triangle}$. Now let $F \in \mathcal{F}(E : K)$. Then, by part 1 of Theorem 2.4, $H = F^{\triangle}$ is strongly finite, decidable subgroup of G and $F = H^{\nabla}$ so that $F \in \mathcal{F}(E)$ and also $F^{\triangle} \in \mathcal{G}(E : K)$.

We also need to show that if $U \in \mathcal{G}(E : K)$ then $U^{\nabla} \in \mathcal{F}(E : K)$. But, by Theorem 2.3, $K^{\triangle} = G$ so that, by Theorem 2.2, we are done.

For 3 Let $K \in \mathcal{F}(E)$. Then, as earlier $K = G^{\nabla}$, where $G = K^{\triangle}$ is strongly finite. Now observe that the following are equivalent.

1. $K \in \mathcal{F}(F)$,

2. $K = \{x \in F \mid \forall h \in H\ h(x) = x\}$ for some strongly finite subgroup H of Aut_F,
3. $K = \{x \in F \mid \forall h \in Gal(F : G^\nabla)\ h(x) = x\}$,
4. $Gal(E : F)$ is a normal subgroup of $Gal(E : K)$

That the first two are equivalent just uses the definition of $\mathcal{F}(F)$. The equivalence of the second with the third uses parts 2 and 3 of Theorem 2.4. Finally the equivalence of the last two uses part 4 of Theorem 2.4. Now we have the equivalence of the first with the last; i.e. we have proved (a). Finally we use part 5 of Theorem 2.4 to get (b).

2.1 Proof of Theorem 2.1

Let $\sigma_1, \ldots, \sigma_n$ be the pairwise apart elements of G. By lemma 8.2 there are $\omega_1, \ldots, \omega_n \in E$ such that the $\sigma_i(\omega_j)$, for $i, j = 1, \ldots, n$, form an invertible $n \times n$ matrix M over E. We show that $\omega_1, \ldots, \omega_n$ form a basis for the vector space $E : G^\nabla$.

Claim 1: *$\omega_1, \ldots, \omega_n$ are linearly independent in $E : G^\nabla$*

Proof: If $\alpha_1, \ldots, \alpha_n \in G^\nabla$ such that

$$\alpha_1\omega_1 + \cdots + \alpha_n\omega_n = 0$$

then, applying $\sigma_1, \ldots, \sigma_n$ in turn to the equation, we get that

$$M\underline{\alpha} = \underline{0},$$

where $\underline{\alpha}$ is the column vector in E^n of $\alpha_1, \ldots \alpha_n$ and $\underline{0}$ is the zero vector in E^n. As M is invertible it follows that $\underline{\alpha} = \underline{0}$; i.e. $\alpha_1 = \cdots = \alpha_n = 0$.

Claim 2: *$\omega_1, \ldots, \omega_n$ spans $E : G^\nabla$.*

Proof: Let $\omega \in E$. Let $\underline{\omega} \in E^n$ be the column vector $\sigma_1(\omega), \ldots, \sigma_n(\omega)$. As M is invertible there is a unique vector $\underline{\alpha}$, with terms $\alpha_1, \ldots, \alpha_n$, such that

$$M\underline{\alpha} = \underline{\omega}.$$

Now let $\sigma \in G$. Then, because G is a group, the compositions $\sigma\sigma_1, \ldots, \sigma\sigma_n$ form a permutation of $\sigma_1, \ldots, \sigma_n$. So applying σ to each of the n equations given as a vector equation above we get the following vector equation, after suitably permuting the rows.

$$M\underline{\alpha}^\sigma = \underline{\omega},$$

where $\underline{\alpha}^\sigma$ is the column vector with terms $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. It follows that

$$\underline{\alpha}^\sigma = \underline{\alpha};$$

i.e. $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, n$. As this is true for all $\sigma \in G$ it follows that $\alpha_1, \ldots, \alpha_n \in G^\nabla$.

Thus we have shown that, in the vector space $E : G^\nabla$, ω is a linear combination of $\omega_1, \ldots, \omega_n$.

2.2 Proof of Theorem 2.2

By Lemma 6.1 U and G/U are finite sets and

$$|G| = |U| \times |G/U|.$$

By Theorem 4.6 U is strongly finite, so that, by Theorem 2.1 both $E : G^{\nabla}$ and $E : U^{\nabla}$ are finite dimensional and

$$|G| = [E : G^{\nabla}],$$
$$|U| = [E : U^{\nabla}].$$

By Theorem 7.5, $U^{\nabla} : G^{\nabla}$ is finite dimensional and

$$[E : G^{\nabla}] = [E : U^{\nabla}] \times [U^{\nabla} : G^{\nabla}].$$

The required equation is now a conseqence of the four equations above.

2.3 Proof of Theorem 2.3

We will prove the theorem using the following result.

Theorem 2.5 *If $E : F$ is a finite dimensional field extension then $F^{\triangle}$ is $[E : F]$-bounded.*

We can now prove that $G = G^{\nabla\triangle}$. By Theorem 2.1 $E : G^{\nabla}$ is finite dimensional and $[E : G^{\nabla}] = |G|$. By Theorem 2.5, with $F = G^{\nabla}$, $G^{\nabla\triangle}$ is $|G|$-bounded. As $G \subseteq G^{\nabla\triangle}$ we may apply Theorem 5.1 to get that $G = G^{\nabla\triangle}$.

Theorem 2.5 is a special case of the following lemma, after relabelling.

Lemma 2.6 *Let K be a subfield of E and let F be a finite dimensional K-subfield of E. Then $Alg_K(F, E)$ is $[F : K]$-bounded.*

2.3.1 Proof of Lemma 2.6

We will first need the following result.

Lemma 2.7 *Let K be a subfield of E and let F be a finite dimensional K-subfield of E. Then, viewing F and E as vector spaces over K let V be the set of K-linear maps $F \to E$. This naturally forms a vector space over E whose dimension is $[F : K]$. Moreover V is pairwise apart.*

Proof: The set E^F of all functions $F \to E$ forms a vector space over E. Let $n = [F : K]$ and let $x_1, \ldots, x_n$ be a basis for the vector space $F : K$ over K. By the following sublemma V is an n-dimensional vector space over E.

Sublemma 2.8

1. *V is a subspace of E^F.*
2. *There are unique functions $\theta_1, \ldots, \theta_n : F \to E$ such that if $a = a_1x_1 + \cdots + a_nx_n$, with $a_1, \ldots, a_n \in K$, then $\theta_i(a) = a_i$.*
3. *$\theta_i \in V$ for $i = 1, \ldots, n$.*

4. $\theta_1, \ldots, \theta_n$ *form a basis for* V.

The proof of this sublemma is routine. We can now rerturn to the proof of Lemma 2.6. Let $n = [F : K]$ and let $g_0, g_1, \ldots, g_n \in Alg_K(F, E)$. Then $g_0, g_1, \ldots, g_n \in V$, where V is as in Lemma 2.7. As V has dimension n, $g_0, g_1, \ldots, g_n$ are linearly dependent and hence cannot be linearly apart. So, by Theorem 8.1, the list $g_0, g_1, \ldots, g_n$ cannot be pairwise apart. But, as V is finite dimensional, it is discrete, so that $\{g_0, g_1, \ldots, g_n\}$ is a finite set and hence a strongly finite set, it is pairwise apart, by the lemma. So the list cannot be pairwise distinct; i.e.

$$\neg \bigwedge_{1 \leq i < j \leq n} g_i \neq g_j.$$

As V is discrete, $g_i = g_j$ for some i, j such that $1 \leq i < j \leq n$.

2.4 Proof of Theorem 2.4

Let $K = G^{\nabla}$ and let F be a finite dimensional K-subfield of E. We will need to prove some preliminary results.

Lemma 2.9 *$F^{\triangle}$ is a decidable subgroup of G, $F^{\triangle}$ and $G \restriction F$ are strongly finite sets of functions, $G/F^{\triangle}$ is finite and*

$$|G/F^{\triangle}| = |G \restriction F|.$$

Proof: By Theorem 2.3 $G = K^{\triangle} \supseteq F^{\triangle}$. Moreover $F^{\triangle}$ is a decidable subgroup of G. To see this let $x_1, \ldots, x_n \in F$ be a basis for $F : K$. Now let $g \in G$. Then

$$g \in F^{\triangle} \Leftrightarrow g(x_i) = x_i \text{ for all } i = 1, \ldots, n$$

and the right hand side is decidable. So by Theorem 4.6, $F^{\triangle}$ is strongly finite. Also observe that $G \restriction F$ is pairwise apart and hence strongly finite if finite. To see this let $g_1, g_2 \in G$ with $g_1 \restriction F \neq g_2 \restriction F$. Then $g_1(x_i) \neq g_2(x_i)$ for some $i = 1, \ldots, n$ so that $g_1 \restriction F$ is apart from $g_2 \restriction F$.

It only remains to define a bijection $\theta : G/F^{\triangle} \to G \restriction F$. First observe that, for $g_1, g_2 \in G$

$$\begin{aligned} g_1 F^{\triangle} = g_2 F^{\triangle} &\Leftrightarrow g_2^{-1} g_1 \in F^{\triangle} \\ &\Leftrightarrow (\forall x \in F)(g_2^{-1} g_1)(x) = x \\ &\Leftrightarrow (\forall x \in F) g_1(x) = g_2(x) \\ &\Leftrightarrow g_1 \restriction F = g_2 \restriction F \end{aligned}$$

It follows that there is a unique bijective function $\theta : G/F^{\triangle} \to G \restriction F$ such that

$$\theta(g F^{\triangle}) = g \restriction F$$

for all $g \in G$.

Theorem 2.10

(i) $G \restriction F = Alg_K(F, E)$.

(ii) $|G \restriction F| = [F : K]$.

(iii) $F = F^{\triangle \nabla}$.

Proof: By Theorem 2.3 $G = K^{\triangle} \supseteq F^{\triangle}$. Moreover $F^{\triangle}$ is a decidable subgroup of G, by Lemma 2.9, so that $F^{\triangle}$ is strongly finite and

$$[F : K] \leq [F^{\triangle\nabla} : K] = |G/F^{\triangle}| = |G \upharpoonright F|$$

using Lemma 2.2 and Lemma 2.9 again. But $G \upharpoonright F \subseteq Alg_K(F, E)$ and, by Lemma 2.6, $Alg_K(F, L)$ is $[F : K]$-bounded. It follows that (i) and

$$[F : K] = [F^{\triangle\nabla} : K] = |G/F^{\triangle}| = |G \upharpoonright F|$$

so that (ii). Finally, for (iii), as $F \subseteq F^{\triangle\nabla}$ and $[F : K] = [F^{\triangle\nabla} : K]$ we get that $F = F^{\triangle\nabla}$.

Corollary 2.11 *$Gal(F : K)$ is strongly finite and the following are equivalent.*

(i) *$F^{\triangle}$ is a normal subgroup of G.*

(ii) *$G \upharpoonright F = Gal(F : K)$.*

(iii) *$|G \upharpoonright F| = |Gal(F : K)|$.*

Proof: Note that, by Theorem 2.10, $Alg_K(F, E) = G \upharpoonright F$, which is strongly finite, Lemma 2.9. So, for $g \in Alg_K(F, E)$,

$$\begin{aligned} g \in Gal(F : K) \quad &\Leftrightarrow \forall x \in F \; g(x) = x \\ &\Leftrightarrow g(x_1), \ldots, g(x_n) \in F \end{aligned}$$

where $x_1, \ldots, x_n$ is a basis for $F : K$. It follows that, as F is a decidable subfield of E by ???, $Gal(F : K)$ is a decidable subset of $Alg_K(F, E)$. So, by Theorem 4.6, $Gal(F : K)$ is strongly finite.

(ii)$\rightarrow$ (iii) Trivial.

(iii)$\rightarrow$(ii) By (i) of Theorem 2.10, $Gal(F : K) \subseteq G \upharpoonright F$, giving the result by Theorem 4.7.

(i)$\leftrightarrow$ (ii)
$F^{\triangle}$ is a normal subgroup of G

$$\begin{aligned} &\Longleftrightarrow \forall h \in F^{\triangle} \forall g \in G \; g^{-1}hg \in F^{\triangle} \\ &\Longleftrightarrow \forall h \in F^{\triangle} \forall x \in F \forall g \in G \; (g^{-1}hg)(x) = x \\ &\Longleftrightarrow \forall h \in F^{\triangle} \forall x \in F \forall g \in G \; h(g(x)) = g(x) \\ &\Longleftrightarrow \forall h \in F^{\triangle} \forall y \in GF \; h(y) = y \\ &\Longleftrightarrow GF \subseteq F^{\triangle\nabla} \\ &\Longleftrightarrow GF \subseteq F \\ &\Longleftrightarrow \forall g \in G \; g \upharpoonright F : F \rightarrow F \\ &\Longleftrightarrow \forall g \in G \; g \upharpoonright F \in Gal(F : K) \\ &\Longleftrightarrow G \upharpoonright F \subseteq Gal(F : K) \\ &\Longleftrightarrow G \upharpoonright F = Gal(F : K). \end{aligned}$$

We now turn to the proof of Theorem 2.4

1. By Lemma 2.9 $F^{\triangle}$ is a strongly finite decidable subgroup of G. By (iii) of Theorem 2.10 $F^{\triangle\nabla} = F$.

2. By Corollary 2.11 $Gal(F, G^{\nabla})$ is strongly finite.

3. Let H be a strongly finite subgroup of Aut_F. Then, by Theorem 2.3, with $E = F$ and $G = H$, $H = Gal(F : F_H)$, where

$$F_H = \{x \in F \mid \forall h \in H \; h(x) = x\}.$$

So if $G^{\nabla} = F_H$ then $H = Gal(F : G^{\nabla}) = G_F$.

4. By Corollary 2.11 $F^{\triangle}$ is a normal subgroup of G if and only if $G \restriction F = Gal(F : G^{\nabla}) = G_F$. But, if $G \restriction F = G_F$ then, as $G^{\nabla} \subseteq F$,

$$\begin{array}{rl} G^{\nabla} = & \{x \in E \mid \forall g \in G \; g(x) = x\} \\ & \{x \in F \mid \forall g \in G \; g(x) = x\} \\ & \{x \in F \mid \forall g \in G_F \; g(x) = x\} \end{array}$$

So we have the implication from right to left. For the converse implication let $G^{\nabla} = \{x \in F \mid \forall g \in G_F \; g(x) = x\}$. Then, by Theorem 2.1, with $E = F$ and $G = G_F$, $[F : G^{\nabla}] = |G_F|$. So, by (ii) of Theorem 2.10, $|G \restriction F| = |G_F|$ and hence, by Corollary 2.11, $F^{\triangle}$ is a normal subgroup of G.

5. Let $F^{\triangle}$ be a normal subgroup of G. Let θ be as in the proof of Lemma 2.9. Observe that it is group isomorphism between the groups $G/F^{\triangle}$ and $G \restriction F = G_F$.

Appendix: Auxilliary results

In this appendix I state some results that are not part of Galois Theory, but are needed in the development of the theory.

3 Logic

A subset X of a set A is a **decidable subset of** A if, for every $a \in A$ either $a \in X$ or $a \notin X$.

Proposition 3.1 *Let A, B be sets and let R be a subset of $A \times B$. If A' is a finite subset of A and*

$$\begin{array}{ll} B_1 & = \{y \in B \mid \forall x \in A' \; xRy\} \\ B_2 & = \{y \in B \mid \exists x \in A' \; xRy\} \end{array}$$

then B_1, B_2 are decidable subsets of B.

A set A is **discrete** if equality on it is decidable; i.e. for $a_1, a_2 \in A$ either $a_1 = a_2$ or $a_1 \neq a_2$. If A, B are sets, with B discrete, then call $h_1, h_2 : A \to B$ **apart** if $h_1(a) \neq h_2(a)$ for some $a \in A$. Note that $h_1 = h_2$ if and only if h_1, h_2 are not apart. Call a subset H of B^A **pairwise apart** if, for all $h_1, h_2 \in H$

$$h_1 \neq h_2 \Longrightarrow h_1 \text{ is apart from } h_2.$$

Proposition 3.2 *Let $H \subseteq B^A$, where B is a discrete set, such that there is a finite subset A' of A such that, for all $h_1, h_2 \in H$*

$$h_1 \restriction A' = h_2 \restriction A' \Rightarrow h_1 = h_2.$$

Then H is a pairwise apart discrete set.

4 Finite Sets

Theorem 4.1 *Any decidable subset of a finite set is finite.*

Theorem 4.2 *Any discrete image of a finite set is finite.*

Theorem 4.3 *If a finite subset of a set has the same number of elements as the set itself then the subset is equal to the set.*

Theorem 4.4 *If X, Y are finite sets and $f : X \to Y$ is surjective then there is a function $g : Y \to X$ such that $f(g(y)) = y$ for all $y \in Y$.*

Definition 4.5 *A finite set of functions $A \to B$, with B discrete, that is pairwise apart, as described in the previous section, is called* **strongly finite**.

Theorem 4.6 *Any decidable subset of a strongly finite set of functions is also strongly finite.*

Theorem 4.7 *If X, Y are finite sets, with $|X| = |Y|$, and $X \subseteq Y$ then $X = Y$.*

5 Sets bounded in number

For a natural number n, a set A is n-**bounded** if whenever $a_0, a_1, \ldots, a_n \in A$ then there are i, j such that $0 \leq i < j \leq n$ and $a_i = a_j$.

Theorem 5.1 *If A is an n-bounded set and $X \subseteq A$ is a finite subset such that $|X| \geq n$ then $X = A$ and $|X| = n$.*

6 Groups

If U is a subgroup of a group G then let $G/U = \{gU \mid g \in G\}$, where $gU = \{gg' \mid g' \in U\}$. Recall that when U is a normal subgroup of G then G/U can be made into a group with group operation given by

$$(gU)(g'U) = (gg')U$$

for all $g, g' \in G$.

Lemma 6.1 *If U is a decidable subgroup of a finite group G then U and G/U are finite and*

$$|G| = |G/U| \times |U|.$$

Theorem 6.2 *If $\theta : G \to H$ is a surjective group homomorphism, from group G to group H, and $ker(\theta) = G'$ then $G/G' \cong H$.*

7 Vector Spaces

7.1 Finite Dimensional Vector Spaces

We first give the standard definition of the notion of a finite dimensional vector space. Let V be a vector space over a field F. If $x_1, \ldots, x_n$ is a list of vectors in V and $a_1, \ldots a_n$ are elements of F then $a_1x_1 + \cdots + a_nx_n$ is a **linear combination** of $x_1, \ldots, x_n$. It is a **non-trivial linear combination** if not all of $a_1, \ldots, a_n$ are 0. A subset X of V is **linearly dependent** if there is a non-trivial linear combination of a pairwise distinct list of elements of X that is not equal to 0. A subset that is not linearly dependent is **linearly independent**. The **span**, $\langle X \rangle$, of a subset X of V, is the set of vectors in V that are linear combinations of elements of X. A **basis** for V is a linearly independent subset of V whose span is equal to V.

Definition 7.1 *A vector space is* **finite dimensional** *if it has a finite basis.*

Theorem 7.2 *Every basis of a given finite dimensional vector space has the same number of elements.*

The number of elements in a basis of a finite dimensional vector space is called the **dimension** of the vector space.

Theorem 7.3 *If V is a finite dimensional vector space, with dimension n, then any subset, with more than n elements, is linearly dependent.*

Theorem 7.4 *In a finite dimensional vector space, with dimension n, any n linearly independent vectors form a basis.*

Theorem 7.5 *Let $F : K$ be a field extension and let V be a non-trivial vector space over F. Then V may be considered as a vector space V_K over K. Any two of the following conditions imply the third and these conditions together imply*

$$(*) \qquad dim(V_K) = [F : K] \times dim(V).$$

1. *$F : K$ is finite dimensional.*
2. *V is finite dimensional.*
3. *V_K is finite dimensional.*

8 Characters

Let E be a field. For any set A the set E^A of functions $A \to E$ forms a vector space over E. Call a subset H of E^A **linearly apart** if any non-trivial linear combination of a pairwise apart list of elements of H is apart from the zero vector in E^A.

Now let A be a multiplicative monoid. The vector $g \in E^A$ is an A**-character for** E if $g : A \to E$ is a monoid homomorphism.

Theorem 8.1 *Any strongly finite set of A-characters for E is linearly apart*

Proof: We prove this by induction on the number n of elements in a strongly finite set of characters. The base, $n = 0$ is trivial, as is the case when $n = 1$, after observing that, for any character g, $g(1) = 1$, so that, for $a \in E$, if $a \neq 0$ then $ag(1) \neq 0$ in E^A.

As induction step, we may assume that the result holds for strongly finite sets of characters having $n-1$ elements where $n > 1$. So let $\{g_1, \ldots, g_n\}$ be a strongly finite set of n distinct characters, $g_1, \ldots, g_n$. Then these are pairwise apart.

Let $p = a_1 g_1 + \cdots + a_n g_n \in E^A$ be a non-trivial linear combination. So $a_1, \ldots, a_n \in E$ are not all 0. It suffices to show that $p(z) \neq 0$ for some $z \in A$. If some $a_i = 0$ then we may use the induction hypothesis. So we may assume without loss that all $a_1, \ldots, a_n$ are non-zero.

Observe that, for $x, y \in A$,

$$g_n(y)p(x) - p(xy) = \sum_{1 \leq i < n} a_i(g_n(y) - g_i(y))g_i(x)$$

Choose $y \in A$ so that $g_n(y) \neq g_1(y)$. Then, as $a_1 \neq 0$,

$$a_1(g_n(y) - g_i(y)) \neq 0.$$

So, by the induction hypothesis

$$g_n(y)p(x) - p(xy) \neq 0$$

for some $x \in A$. So one of $p(x) \neq 0$ or $p(xy) \neq 0$. In each case we can choose $z \in A$ so that $p(z) \neq 0$. So we are done.

Note: It is also possible to prove the variant result that any discrete set of A-characters are linearly independent. This variant does not seem to be a direct consequence of the theorem. Anyway we will not need it. The following result will be useful.

Lemma 8.2 *If $\sigma_1, \ldots, \sigma_n \in Aut_E$ are pairwise apart then there are $\omega_1, \ldots, \omega_n \in E$ such that the $n \times n$ matrix, with $\sigma_i(\omega_j)$ in the ij position, is invertible.*

Proof: This is by induction on $n > 0$. When $n = 1$ we can choose $\omega_1 = 1$. For the induction step we assume that the result is true for a given $n > 0$. Let $\sigma_1, \ldots, \sigma_{n+1} \in Aut_E$ be pairwise apart. Then, by the induction hypothesis we can choose $\omega_1, \ldots, \omega_n \in E$ such that the $n \times n$ matrix of terms $\sigma_i(\omega_j)$ for $1 \leq i, j \leq n$ is invertible. It follows that there are $\alpha_1, \ldots, \alpha_n \in E$ such that

$$\sigma_{n+1}(\omega_j) = \sum_{i=1}^{n} \alpha_i \sigma_i(\omega_j)$$

for $j = 1, \ldots, n$. By Theorem 8.1 there is $\omega_{n+1} \in E$ such that $a \neq 0$ where

$$a = \sigma_{n+1}(\omega_{n+1}) - \sum_{i=1}^{n} \alpha_i \sigma_i(\omega_{n+1}).$$

We now show that the $(n+1) \times (n+1)$ matrix of terms $\sigma_i(\omega_j)$ for $1 \leq i, j \leq n+1$ is invertible. Let

$$v_i = (\sigma_i(\omega_1), \ldots, \sigma_i(\omega_{n+1})) \in E^{n+1}$$

for $i = 1, \ldots, n+1$. Note that

$$v_{n+1} = a^{n+1} + \sum_{i=1}^{n} \alpha_i v_i,$$

where $a^{n+1} = (0, \ldots, 0, a) \in E^{n+1}$.

By Theorem 7.4 it suffices to show that the vectors $v_1, \ldots, v_{n+1}$ are linearly independent in E^{n+1}. Let

$$v_i^- = (\sigma_i(\omega_1), \ldots, \sigma_i(\omega_n)) \in E^n.$$

then $v_1^-, \ldots, v_n^-$ are linearly independent in E^n and

$$v_{n+1}^- = \sum_{i=1}^{n} \alpha_i v_i^-.$$

Now let

$$\sum_{i=1}^{n+1} \beta_i v_i = 0^{n+1},$$

where $\beta_i \in E$ for $i = 1, \ldots, n+1$ and $0^k \in E^k$ is the zero vector for any $k \in \mathbb{N}$. Then

$$\sum_{i=1}^{n} \beta_i v^i + \beta_{n+1}(a^{n+1} + \sum_{i=1}^{n} \alpha_i v_i) = 0^{n+1},$$

so that

$$\sum_{i=1}^{n} \beta_i' v_i + \beta_{n+1} a^{n+1} = 0^{n+1},$$

where $\beta_i' = \beta_i + \beta_{n+1}\alpha_i$ for $i = 1, \ldots, n$. By projecting onto E^n and onto E we get that $\sum_{i=1}^{n} \beta_i' v_i^- = 0^n$ and

$$\sum_{i=1}^{n} \beta_i' \sigma_i(\omega_{n+1}) + \beta_{n+1} a = 0.$$

As $v_1^-, \ldots, v_n^-$ are linearly independent, $\beta_i' = 0$ for $i = 1, \ldots, n$. So, as $a \neq 0$, $\beta_{n+1} = 0$ and hence $\beta_i = \beta_i + \beta_{n+1}\alpha_i = \beta_i' = 0$ for $i = 1, \ldots, n$

Thus we have shown that $v_1, \ldots, v_{n+1}$ are linearly independent, as required.