Chapter 1.
Algebraic Patching

Let E be a field, G a finite group, and $\{G_i \mid i \in I\}$ a finite set of subgroups of G with $G = \langle G_i \mid i \in I\rangle$. For each $i \in I$ we are given a Galois extension F_i of E with Galois group G_i. We suggest a general method how to 'patch' the given F_i's into a Galois extension F with Galois group G (Lemma 1.1.7). Our method requires extra fields P_i, all contained in a common field Q and satisfying certain conditions making $\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i\in I}$ into 'patching data' (Definition 1.1.1). The auxiliary fields P_i in this data substitute, in some sense, analytic fields in rigid patching and fields of formal power series in formal patching.

If in addition to the patching data, E is a Galois extension of a field E_0 with Galois group Γ and Γ 'acts properly' (Definition 1.2.1) on the patching data $\mathcal{E}$, then we construct F above to be a Galois extension of E_0 with Galois group isomorphic to $\Gamma \ltimes G$ (Proposition 1.2.2).

1.1 Patching

Let E be a field and G a finite group, generated by finitely many subgroups G_i, $i \in I$. Suppose for each $i \in I$ we have a finite Galois field extension F_i of E with Galois group G_i. We use these extensions to construct a Galois field extension F of E (not necessarily containing F_i) with Galois group G. First we 'lift' each F_i/E to a Galois field extension Q_i/P_i, where P_i is an appropriate field extension of E such that $P_i \cap F_i = E$ and all of the Q_i's are contained in a common field Q. Then we define F to be the maximal subfield contained in $\bigcap_{i\in I} Q_i$ on which the Galois actions of $\mathrm{Gal}(Q_i/P_i)$ combine to an action of G.

The construction works if certain patching conditions on the initial data are satisfied.

Definition 1.1.1: Patching data. Let I be a finite set with $|I| \geq 2$. A **patching data**

$$\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i\in I}$$

consists of fields $E \subseteq F_i, P_i \subseteq Q$ and finite groups $G_i \leq G$, $i \in I$, such that

(1a) F_i/E is a Galois extension with Galois group G_i, $i \in I$;

(1b) $F_i \subseteq P_i'$, where $P_i' = \bigcap_{j\neq i} P_j$, $i \in I$;

(1c) $\bigcap_{i\in I} P_i = E$; and

(1d) $G = \langle G_i \mid i \in I\rangle$.

(1e) (Cartan's decomposition) Let $n = |G|$. Then for every $B \in \mathrm{GL}_n(Q)$ and each $i \in I$ there exist $B_1 \in \mathrm{GL}_n(P_i)$ and $B_2 \in \mathrm{GL}_n(P_i')$ such that $B = B_1 B_2$. □

M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics,
DOI 10.1007/978-3-642-15128-6_1, © Springer-Verlag Berlin Heidelberg 2011

We extend $\mathcal{E}$ by more fields. For each $i \in I$ let $Q_i = P_iF_i$ be the compositum of P_i and F_i in Q. Conditions (1b) and (1c) imply that $P_i \cap F_i = E$. Hence Q_i/P_i is a Galois extension with Galois group isomorphic (via the restriction of automorphisms) to $G_i = \mathrm{Gal}(F_i/E)$. We identify $\mathrm{Gal}(Q_i/P_i)$ with G_i via this isomorphism.

We need some auxiliary results from linear algebra. Let

$$N = \Big\{ \sum_{\zeta\in G} a_\zeta \zeta \mid a_\zeta \in Q \Big\} \tag{2}$$

be the vector space over Q with basis $(\zeta \mid \zeta \in G)$, where G is given some fixed ordering. Thus $\dim_Q N = |G|$. For each $i \in I$ we consider the following subset of N:

$$N_i = \Big\{ \sum_{\zeta\in G} a_\zeta \zeta \in N \mid a_\zeta \in Q_i,\ a_\zeta^\eta = a_{\zeta\eta} \text{ for all } \zeta \in G,\ \eta \in G_i \Big\}. \tag{3}$$

It is a vector space over P_i.

Lemma 1.1.2: *Let $i \in I$. Then N has a Q-basis which is contained in N_i.*

Proof: Let $\Lambda = \{\lambda_1, \ldots, \lambda_m\}$ be a system of representatives of G/G_i and let $\eta_1, \ldots, \eta_r$ be a listing of the elements of G_i. Thus, $G = \{\lambda_k\eta_\nu \mid k = 1, \ldots, m;\ \nu = 1, \ldots, r\}$. Let z be a primitive element for Q_i/P_i. The following sequence of $|G|$ elements of N_i

$$\Big(\sum_{\nu=1}^{r} (z^{j-1})^{\eta_\nu}\ \lambda_k\eta_\nu \mid j = 1, \ldots, r;\ k = 1, \ldots, m \Big)$$

(in some order) is linearly independent over Q, hence it forms a basis of N over Q.

Indeed, let $a_{jk} \in Q$ such that $\sum_{j=1}^{r}\sum_{k=1}^{m} a_{jk}\big(\sum_{\nu=1}^{r}(z^{j-1})^{\eta_\nu}\ \lambda_k\eta_\nu\big) = 0$. Then

$$\sum_{k=1}^{m}\sum_{\nu=1}^{r}\big(\sum_{j=1}^{r} a_{jk}(z^{j-1})^{\eta_\nu}\ \big)\lambda_k\eta_\nu = 0.$$

This gives $\sum_{j=1}^{r} a_{jk}(z^{j-1})^{\eta_\nu} = 0$ for all k, ν. Thus, for each k, $(a_{1k}, \ldots, a_{rk})$ is a solution of the homogeneous system of equations with the Vandermonde matrix $\big((z^{j-1})^{\eta_\nu}\big)$. Since this matrix is invertible, $a_{jk} = 0$ for all j, k. □

Lemma 1.1.3 (Common lemma): *N has a Q-basis in $\bigcap_{i\in I} N_i$.*

Proof: Consider a nonempty subset J of I. By induction on $|J|$ we find a Q-basis in $\bigcap_{j\in J} N_j$. For $J = I$ this gives the assertion of the lemma.

For each $i \in I$, Lemma 1.1.2 gives a Q-basis $\mathbf{v}_i$ of N in N_i, so the result follows when $|J| = 1$. Assume $|J| \geq 2$ and fix $i \in J$. By induction N has a

Q-basis $\mathbf{u}$ in $\bigcap_{j\in J\smallsetminus\{i\}} N_j$. The transition matrix $B\in \mathrm{GL}_n(Q)$ between $\mathbf{v}_i$ and $\mathbf{u}$ satisfies

$$\mathbf{u}=\mathbf{v}_iB. \tag{4}$$

By (1e), there exist $B_1\in \mathrm{GL}_n(P_i)$ and $B_2\in \mathrm{GL}_n(P_i')\subseteq \bigcap_{j\in J\smallsetminus\{i\}}\mathrm{GL}_n(P_j)$. such that $B=B_1B_2$. Then $\mathbf{u}B_2^{-1}=\mathbf{v}_iB_1$ is a Q-basis of N in $\bigcap_{j\in J}N_j$. This finishes the induction. □

We introduce a special subset F of $\bigcap_{i\in I}Q_i$, call it the 'compound of the special data $\mathcal{E}$', and prove that F is a Galois extension of E with Galois group G and additional properties.

Definition 1.1.4: Compound. The **compound** of the patching data $\mathcal{E}$ is the set F of all $a\in\bigcap_{i\in I}Q_i$ for which there exists a function $f\colon G\to\bigcap_{i\in I}Q_i$ such that
(5a) $a=f(1)$ and
(5b) $f(\zeta\tau)=f(\zeta)^\tau$ for every $\zeta\in G$ and $\tau\in\bigcup_{i\in I}G_i$.

Note that for each $a\in\bigcap_{i\in I}Q_i$, the function f is uniquely determined by (5a) and (5b). Indeed, let $f'\colon G\to\bigcap_{i\in I}Q_i$ be another function such that $f'(1)=1$ and $f(\zeta\tau)=f(\zeta)^\tau$ for all $\zeta\in G$ and $\tau\in\bigcup_{i\in I}G_i$. In particular, $f'(1)=f(1)$. By (1d), each $\sigma\in G$, $\sigma\neq 1$, can be written as $\sigma=\tau_1\cdots\tau_m$ with $\tau_i\in\bigcup_{i\in I}G_i$, $i=1,\ldots,m$, and $m\geq 1$. Set $\zeta=\tau_1\cdots\tau_{m-1}$ and $\tau=\tau_m$. By induction on m we assume that $f'(\zeta)=f(\zeta)$. Then $f'(\sigma)=f'(\zeta)^\tau=f(\zeta)^\tau=f(\sigma)$.

We call f the **expansion** of a and denote it by f_a. Thus, $f_a(1)=a$ and $f_a(\zeta\tau)=f_a(\zeta)^\tau$ for all $\zeta\in G$ and $\tau\in\bigcup_{i\in I}G_i$. □

We list some elementary properties of the expansions:

Lemma 1.1.5: *Let F be the compound of $\mathcal{E}$. Then:*
(a) *Every $a\in E$ has an expansion, namely the constant function $\zeta\mapsto a$.*
(b) *Let $a,b\in F$. Then $a+b, ab\in F$; in fact, $f_{a+b}=f_a+f_b$ and $f_{ab}=f_af_b$.*
(c) *Let $0\neq a\in F$, then $a^{-1}\in F$. More precisely: $f_a(\zeta)\neq 0$ for all $\zeta\in G$, and $\zeta\mapsto f_a(\zeta)^{-1}$ is the expansion of a^{-1}.*
(d) *Let $a\in F$ and $\sigma\in G$. Then $f_a(\sigma)\in F$; in fact, $f_{f_a(\sigma)}(\zeta)=f_a(\sigma\zeta)$.*

Proof: Statement (a) holds, because $a^\tau=a$ for each $\tau\in\bigcup_{i\in I}G_i$. Statement (b) follows from the uniqueness of the expansions and from the observation $(f_{a+b})(1)=a+b=f_a(1)+f_b(1)=(f_a+f_b)(1)$.

Next we consider a nonzero $a\in F$ and let $\zeta\in G$. Using (1d), we write $\zeta=\tau_1\cdots\tau_m$ with $\tau_1,\ldots,\tau_m\in\bigcup_{i\in I}G_i$ and set $\zeta'=1$ if $m=1$ and $\zeta'=\tau_1\cdots\tau_{m-1}$ if $m\geq 2$. If $m=1$, then $f_a(\zeta')=a\neq 0$, by assumption. If $m\geq 2$, then $f_a(\zeta')\neq 0$, by an induction hypothesis. In each case, $f_a(\zeta)=f_a(\zeta')^{\tau_m}\neq 0$. Since taking inverse in $\bigcap_{i\in I}Q_i$ commutes with the action of G, the map $\zeta\mapsto f_a(\zeta)^{-1}$ is the expansion of a^{-1}. This proves (c).

Finally, we check that the map $\zeta \to f_a(\sigma\zeta)$ has the value $f_a(\sigma)$ at $\zeta = 1$ and it satisfies (5b). Hence, that map is an expansion of $f_a(\sigma)$, as claimed in (d). □

Definition 1.1.6: G-action on F. For $a \in F$ and $\sigma \in G$ put

$$a^\sigma = f_a(\sigma), \qquad (6)$$

where f_a is the expansion of a. □

LEMMA 1.1.7: *The compound F of the patching data $\mathcal{E}$ is a Galois field extension of E with Galois group G acting by (6). Moreover, for each $i \in I$,*

(a) *the restriction of this action to G_i coincides with the action of $G_i = \mathrm{Gal}(Q_i/P_i)$ on F as a subset of Q_i*

(b) *and $Q_i = P_iF$.*

Proof: By Lemma 1.1.5(a),(b),(c), F is a field containing E. Furthermore, (6) defines an action of G on F. Indeed, if $a \in F$ and $\sigma, \zeta \in G$, then by Lemma 1.1.5(d), $(a^\sigma)^\zeta = f_a(\sigma)^\zeta = f_{f_a^\sigma}(\zeta) = f_a(\sigma\zeta) = a^{(\sigma\zeta)}$.

Proof of (a): Let $\tau \in G_i$ and $a \in F$. Then $f_a(\tau) = f_a(1)^\tau = a^\tau$, where τ acts as an element of $G = \mathrm{Gal}(Q_i/P_i)$. Thus, that action coincides with the action given by (6).

The rest of the proof of (a) breaks up into three parts.

PART A: *$F^G = E$.* Indeed, by Lemma 1.1.5(a), elements of E have constant expansions, hence are fixed by G. Conversely, let $a \in F^G$. Then for each $i \in I$ we have $a \in Q_i^{G_i} = P_i$. Hence, by (1c), $a \in E$.

PART B: *$[F : E] \geq |G|$.* We define a map T: $F \to N$ by

$$T(a) = \sum_{\zeta \in G} f_a(\zeta)\zeta.$$

By Lemma 1.1.5(a),(b), T is an E-linear map, and $\mathrm{Im}(T) = \bigcap_{i \in I} N_i$. By Lemma 1.1.3, $\mathrm{Im}(T)$ contains $|G|$ linearly independent elements over Q, hence over E. Therefore, $[F : E] = \dim_E F \geq |G|$.

PART C: *F/E is Galois and* $\mathrm{Gal}(F/E) = G$. The action (6) of G on F maps G onto a subgroup $\bar{G}$ of $\mathrm{Aut}(F/E)$. By Part A, $F^{\bar{G}} = E$. Hence, by Galois theory, F/E is a Galois extension with Galois group $\bar{G}$. In particular, $[F : E] = |\bar{G}| \leq |G|$. By Part B, $[F : E] \geq |G|$, Hence $G \cong \bar{G}$. So, we may (and we will) identify $\mathrm{Gal}(F/E)$ with G.

Proof of (b): By (a), the restriction $\mathrm{Gal}(Q_i/P_i) \to \mathrm{Gal}(F/E)$ is injective. Hence $Q_i = P_iF$. □

Remark 1.1.8: The vector spaces N and N_i defined by (2) and (3) are actually induced from Q and P_i, respectively, namely $N = \mathrm{Ind}_1^G Q$ and $N_i = \mathrm{Ind}_{G_i}^G Q_i$. We may define multiplication on N componentwise:

$$\sum_{\zeta\in G} a_\zeta \zeta \sum_{\zeta\in G} b_\zeta \zeta = \sum_{\zeta\in G} a_\zeta \beta_\zeta \zeta.$$

Then N becomes a Q-Algebra and N_i becomes a P_i-algebra. By Lemma 1.1.5, the map T: $F \to \bigcap_{i\in I} N_i$ defined in Part B of the proof of Lemma 1.1.7, is an E-linear isomorphism of E-algebras whose inverse is the map $\sum_{\zeta\in G} a_\zeta\zeta \mapsto a_1$. Hence, by that lemma, $F' = \bigcap_{i\in I} N_i$ is a Galois extension of E with Galois group G. The following diagram describes the respective location of all fields and algebras mentioned in our construction:

(7)
$$\begin{tikzcd}
 & N_i \arrow[rrr, dash] \arrow[ld, dash] \arrow[d, dash] & & & N \arrow[ld, dash] \\
P_i \arrow[rr, dash, "G_i"] \arrow[d, dash] & {} \arrow[d, dash] & Q_i \arrow[r, dash] \arrow[d, dash] \arrow[dd, dash, bend left] & Q \arrow[dd, dash] & \\
 & F' \arrow[ld, dash] & F \arrow[l, "T"'] \arrow[lld, dash] & & \\
E \arrow[rr, dash, "G_i"] & & F_i \arrow[r, dash] & P_i' &
\end{tikzcd}$$

$\square$

1.2 Galois Action on Patching Data

A **finite split embedding problem** over a field E_0 is an epimorphism

(1) $$\mathrm{pr}\colon \Gamma \ltimes G \to \Gamma$$

of finite groups, where $\Gamma = \mathrm{Gal}(E/E_0)$ is the Galois group of a Galois extension E/E_0, G is a finite group on which Γ acts from the right, $\Gamma \ltimes G$ is the corresponding semidirect product, and pr is the projection on Γ. Each element of $\Gamma \ltimes G$ has a unique representation as a product $\gamma\zeta$ with $\gamma \in \Gamma$ and $\zeta \in G$. The product and the inverse operation are given in $\Gamma \ltimes G$ by the formulas $\gamma\zeta \cdot \delta\eta = \gamma\delta \cdot \zeta^\delta \eta$ and $(\gamma\zeta)^{-1} = \gamma^{-1}(\zeta^{\gamma^{-1}})^{-1}$. A **solution** of (1) is a Galois extension F of E_0 that contains E and an isomorphism ψ: $\mathrm{Gal}(F/E_0) \to \Gamma \ltimes G$ such that $\mathrm{pr} \circ \psi = \mathrm{res}_E$. We call F a **solution field** of (1).

Suppose the compound F of a patching data $\mathcal{E}$ (§1.1) realizes G over E. A 'proper' action of Γ on $\mathcal{E}$ will then ensure that F is even a solution field for the embedding problem (1).

Definition 1.2.1: Let E/E_0 be a finite Galois extension with Galois group Γ. Let $\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i\in I}$ be a patching data (Definition 1.1.1). A **proper action** of Γ on $\mathcal{E}$ is a triple that consists of an action of Γ on the group G, an action of Γ on the field Q, and an action of Γ on the set I such that the following conditions hold:

(2a) The action of Γ on Q extends the action of Γ on E.

(2b) $F_i^\gamma = F_{i^\gamma}$, $P_i^\gamma = P_{i^\gamma}$, and $G_i^\gamma = G_{i^\gamma}$, for all $i \in I$ and $\gamma \in \Gamma$.

(2c) $(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma}$ for all $i \in I$, $a \in F_i$, $\tau \in G_i$, and $\gamma \in \Gamma$.

The action of Γ on G defines a semidirect product $\Gamma \ltimes G$ such that $\tau^\gamma = \gamma^{-1}\tau\gamma$ for all $\tau \in G$ and $\gamma \in \Gamma$. Let pr: $\Gamma \ltimes G \to \Gamma$ be the canonical projection. □

Proposition 1.2.2: *In the notation of Definition 1.2.1 suppose that* $\Gamma = \mathrm{Gal}(E/E_0)$ *acts properly on the patching data* $\mathcal{E}$ *given in Definition 1.2.1. Let* F *be the compound of* $\mathcal{E}$*. Then* Γ *acts on* F *via the restriction from its action on* Q *and the actions of* Γ *and* G *on* F *combine to an action of* $\Gamma \ltimes G$ *on* F *with fixed field* E_0*. This gives an identification* $\mathrm{Gal}(F/E_0) = \Gamma \ltimes G$ *such that the following diagram of short exact sequences commutes:*

$$\begin{tikzcd}
1 \arrow[r] & G \arrow[r] \arrow[d, equal] & \Gamma \ltimes G \arrow[r, "\mathrm{pr}"] \arrow[d, equal] & \Gamma \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathrm{Gal}(F/E) \arrow[r] & \mathrm{Gal}(F/E_0) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(E/E_0) \arrow[r] & 1
\end{tikzcd}$$

Thus, F *is a solution field of the embedding problem (1).*

Proof: We break the proof of the proposition into three parts.

Part A: *The action of* Γ *on* F.

Let $i \in I$ and $\gamma \in \Gamma$. Then $Q_i = P_iF_i$, so by (2b), $Q_i^\gamma = Q_{i^\gamma}$. Moreover, we have identified $\mathrm{Gal}(Q_i/P_i)$ with $G_i = \mathrm{Gal}(F_i/E)$ via restriction. Hence, by (2b), for all $a \in P_i$ and $\tau \in G_i$ we have $\tau^\gamma \in G_{i^\gamma}$ and $a^\gamma \in P_{i^\gamma}$, so $(a^\tau)^\gamma = a^\gamma = (a^\gamma)^{\tau^\gamma}$. Together with (2c), this gives

$$(a^\tau)^\gamma = (a^\gamma)^{\tau^\gamma} \qquad \text{for all } a \in Q_i \text{ and } \tau \in G_i. \tag{4}$$

Consider an $a \in F$ and let f_a be the expansion of a (Definition 1.1.4). Define f_a^γ: $G \to \bigcap_{i\in I} Q_i$ by $f_a^\gamma(\zeta) = f_a(\zeta^{\gamma^{-1}})^\gamma$. Then f_a^γ is the expansion f_{a^γ} of a^γ. Indeed, $f_a^\gamma(1) = f_a(1^{\gamma^{-1}})^\gamma = a^\gamma$ and if $\zeta \in G$ and $\tau \in G_i$, then $\tau^{\gamma^{-1}} \in G_{i^{\gamma^{-1}}}$. Hence, by (4) with $i^{\gamma^{-1}}, f_a(\zeta^{\gamma^{-1}}), \tau^{\sigma^{-1}}$, respectively, replacing i, a, τ, we have

$$\begin{aligned} f_a^\gamma(\zeta\tau) = f_a(\zeta^{\gamma^{-1}}\tau^{\gamma^{-1}})^\gamma &= \big(f_a(\zeta^{\gamma^{-1}})^{\tau^{\gamma^{-1}}}\big)^\gamma \\ &= \big(f_a(\zeta^{\gamma^{-1}})^\gamma\big)^{\tau^{\gamma^{-1}\gamma}} = \big(f_a(\zeta^{\gamma^{-1}})^\gamma\big)^\tau = f_a^\gamma(\zeta)^\tau. \end{aligned}$$

Thus $a^\gamma \in F$. It follows that the action of Γ on Q gives an action of Γ on F.

Part B: *The action of* $\Gamma \ltimes G$ *on* F. Let $a \in F$ and $\gamma \in \Gamma$. We claim that

$$(a^\sigma)^\gamma = (a^\gamma)^{\sigma^\gamma} \qquad \text{for all } \sigma \in G, \tag{5}$$

where $a^\sigma = f_a(\sigma)$ (Definition 1.1.6). Indeed, write σ as a word in $\bigcup_{i\in I} G_i$. Then (5) follows from (4) by induction on the length of the word. If $\sigma = 1$, then (5) is an identity. Suppose (5) holds for some $\sigma \in G$ and let $\tau \in \bigcup_{i\in I} G_i$. Using the identification of the action of each $\tau \in G_i$ on F as an element of G_i with its action as an element of G (Lemma 1.1.7(a)) and (4) for a^σ rather that a, we have

$$(a^{\sigma\tau})^\gamma = \big((a^\sigma)^\tau\big)^\gamma = \big((a^\sigma)^\gamma\big)^{\tau^\gamma} = \big((a^\gamma)^{\sigma^\gamma}\big)^{\tau^\gamma} = (a^\gamma)^{\sigma^\gamma\tau^\gamma} = (a^\gamma)^{(\sigma\tau)^\gamma}.$$

Now we apply (5) to $a^{\gamma^{-1}}$ instead of a to find that $\Big(\big(a^{\gamma^{-1}}\big)^\sigma\Big)^\gamma = a^{\sigma^\gamma}$. It follows that the actions of Γ and G on F combine to an action of $\Gamma \ltimes G$ on F.

$$\begin{tikzcd}
 & P_i \arrow[r, dash] \arrow[dd, dash] & Q_i \arrow[r, dash] \arrow[d, dash] \arrow[dd, dash, bend left] & Q \arrow[dd, dash] \\
 & & F \arrow[dl, dash] & \\
E_0 \arrow[r, dash] & E \arrow[r, dash] & F_i \arrow[r, dash] & P_i'
\end{tikzcd} \tag{6}$$

Part C: *Conclusion of the proof.* Since $F^G = E$ (Lemma 1.1.7) and $E^\Gamma = E_0$, we have $F^{\Gamma\ltimes G} = E_0$. Furthermore, $[F : E_0] = [F : E] \cdot [E : E_0] = |G| \cdot |\Gamma| = |G \rtimes \Gamma|$. By Galois theory, $\mathrm{Gal}(F/E_0) = \Gamma \ltimes G$ and the map res: $\mathrm{Gal}(F/E_0) \to \mathrm{Gal}(E/E_0)$ coincides with the canonical map pr: $\Gamma \ltimes G \to \Gamma$. □

1.3 The Compound of the Patching Data

This section offers additional useful information about the patching data $\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i\in I}$ and the diagram (5) of §1.2.

Lemma 1.3.1: *Let F be the compound of the patching data $\mathcal{E}$. Then:*

(a) *Suppose $1 \in I$, $G = G_1 \ltimes H$ and $H = \langle G_i \mid i \in I \smallsetminus \{1\}\rangle$. Then, $F_1 = F^H$ and the identification $\mathrm{Gal}(F/E) = G$ of Lemma 1.1.7 gives the following commutative diagram of short exact sequences:*

$$\begin{tikzcd}
1 \arrow[r] & H \arrow[r] \arrow[d, equal] & G = G_1 \ltimes H \arrow[r, "\mathrm{pr}"] \arrow[d, equal] & G_1 \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & \mathrm{Gal}(F/F_1) \arrow[r] & \mathrm{Gal}(F/E) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(F_1/E) \arrow[r] & 1
\end{tikzcd}$$

(b) *If, in addition to the assumptions of (a), E is a finite Galois extension of a field E_0 with Galois group Γ that acts properly on $\mathcal{E}$ such that $1^\gamma = 1$ for each $\gamma \in \Gamma$, then F is a Galois extension of E_0, F_1, Q_1, and G_1 are Γ-invariant, F_1/E_0 is Galois, and we can identify groups as in the following commutative diagram:*

$$\begin{tikzcd}
\mathrm{Gal}(F_1/E_0) \ltimes H \arrow[rr, "\mathrm{pr}"] \arrow[d, equal] & & \mathrm{Gal}(F_1/E_0) \arrow[d, "\mathrm{res}"] \\
\Gamma \ltimes G \arrow[r, "\mathrm{id}\times\mathrm{pr}"] \arrow[d, equal] & \Gamma \ltimes G_1 \arrow[r, "\mathrm{pr}"] \arrow[d, equal] & \Gamma \arrow[d, equal] \\
\mathrm{Gal}(F/E_0) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(F_1/E_0) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(E/E_0)
\end{tikzcd}$$

Proof of (a): The proof breaks up into several parts.

Part A: $F_1 \subseteq \bigcap_{i\in I} Q_i$. Indeed, $F_1 \subseteq F_1P_1 = Q_1$ and $F_1 \subseteq P_i \subseteq Q_i$ for $i \neq 1$, by Condition (1b) of Section 1.1.

Part B: $F_1 \subseteq F$. Let $a \in F_1$. Then $a^\sigma \in F_1 \subseteq \bigcap_{i\in I} Q_i$ for every $\sigma \in G_1$. Every $\zeta \in G$ has a unique presentation $\zeta = \sigma\eta$, where $\sigma \in G_1$ and $\eta \in H$. Use this to define a function $f\colon G \to \bigcap_{i\in I} Q_i$ by $f(\sigma\eta) = a^\sigma$. We prove that $f = f_a$ is the expansion of a.

First note that $f(1) = a$. Fix $\sigma \in G_1$ and $\eta \in H$ and let $i \in I$ and $\tau \in G_i$. If $i = 1$, then $\sigma\eta\tau = (\sigma\tau)\eta^\tau$, $\sigma\tau \in G_1$, and $\eta^\tau \in H$. Hence $f(\sigma\eta\tau) = a^{\sigma\tau} = (a^\sigma)^\tau = f(\sigma\eta)^\tau$. If $i \neq 1$, then $\sigma\eta\tau = \sigma(\eta\tau)$, $\sigma \in G_1$, and $\eta\tau \in H$. Also, $a^\sigma \in F_1 \subseteq P_i = Q_i^{G_i}$, so $(a^\sigma)^\tau = a^\sigma$. Hence $f(\sigma\eta\tau) = a^\sigma = (a^\sigma)^\tau = f(\sigma\eta)^\tau$. Thus, in both cases $f(\sigma\eta\tau) = f(\sigma\eta)^\tau$. It follows from Definition 1.1.4 that $f = f_a$.

Part C: $a^\tau = a^{\mathrm{pr}(\tau)}$ *for all* $a \in F_1$ *and* $\tau \in G$. Since pr is a homomorphism, it suffices to prove the equality for each τ in a set of generators of G. So we may assume that $\tau \in G_i$ for some $i \in I$. If $i = 1$, then $\mathrm{pr}(\tau) = \tau$ and the assertion follows. If $i \neq 1$, then $\mathrm{pr}(\tau) = 1$, whence $a^{\mathrm{pr}(\tau)} = a$. Moreover, $a \in F_1 \subseteq P_i = Q_i^{G_i}$, so $a^\tau = a$, as claimed.

Part D: *Completion of the proof.* Part C says that res: $\mathrm{Gal}(F/E) \to \mathrm{Gal}(F_1/E)$ and pr: $G \to G_1$ coincide. Hence, the $H = \mathrm{Gal}(F/F_1)$, $F_1 = F^H$, and the diagram in (c) commutes.

Proof of (b): Note that $F_1^\gamma = F_{1^\gamma} = F_1$ and similarly $Q_1^\gamma = Q_1$ and $G_1^\gamma = G_1$ for each $\gamma \in \Gamma$. Thus, $\Gamma \ltimes G_1$ is a subgroup of $\Gamma \ltimes G = \mathrm{Gal}(F/E_0)$ that leaves F_1 invariant. The fixed field of $\Gamma \ltimes G_1$ in F_1 is E_0. Since $|\Gamma \ltimes G_1| = [F_1 : E_0]$, this implies by Galois theory that F_1/E_0 is Galois with Galois group $\Gamma \ltimes G_1$. The identification $\mathrm{Gal}(F_1/E_0) = \Gamma \ltimes G_1$ restricts further to $\mathrm{Gal}(E/E_0) = \Gamma$. This completes the commutativity of the lower part of the diagram in (b).

Since each $\gamma \in \Gamma$ fixes 1 it leaves $I \smallsetminus \{1\}$ invariant, so Γ leaves $H = \langle G_i \mid i \in I \smallsetminus \{1\}\rangle$ invariant. Thus, H can be considered as a normal subgroup of $\Gamma \ltimes G$ with $(\Gamma \ltimes G)/H = \Gamma \ltimes G_1$. To prove the commutativity of the upper part just note that $\Gamma \ltimes G = \Gamma \ltimes (G_1 \ltimes H) = (\Gamma \ltimes G_1) \ltimes H = \mathrm{Gal}(F_1/E_0) \ltimes H$. □

Notes

We call the field $F' = \bigcap_{i\in I} N_i$ that appears in Remark 1.1.8 the **precompound** of the patching data $\mathcal{E}$ of Definition 1.1.1. The idea of a patching data as well as the notions of a 'precompound' and 'compound' of $\mathcal{E}$ appear in [HaV96, Sec. 3] (however, the precompound is denoted by F while the compound is denoted by F' in [HaV96]). It is used there in order to prove that if R is a complete local integral domain which is not a field and if $K = \mathrm{Quot}(R)$, then for every finite group G, the field $K(x)$ has a Galois extension F with Galois group G such that F is a regular extension of K and has a prime divisor of degree 1 unramified over $K(x)$ [HaV96, Thm. 4.4]. In addition, [HaV96, Cor. 4.7] states that if E is a function field of one variable over a countable algebraically closed field, then $\mathrm{Gal}(E) \cong \hat{F}_\omega$.

The action of a finite group on a patching data $\mathcal{E}$ is introduced in [HaJ98a] in order to prove that the precompounds are solution fields of finite split embedding problems [HaJ98a, Prop. 1.5]. This suffices to prove the main theorem of [HaJ98a] that every PAC Hilbertian field is ω-free. Note however, that [HaJ98a] calls a 'compound' what we call a 'precompound'.

The main advantage of the compound F on the precompound F' is that $P_iF = Q_i$ for each $i \in I$. This implies that the set of 'branch points' of F/E_0 is the union of the sets of branch points of F_i/E_0 (Proposition 7.2.3).

The presentation of the compound in Definition 1.1.4 is direct. Thus, we prove the properties of the compound, in particular the solvability of finite split embedding problems, without proving them first for the precompound (as is done in [HaV96] and [HaJ98a]). This shorter presentation is due to Dan Haran (private communication).

Lemma 1.1.3 is a workout of [HaV96, Prop. 3.4] for $|I| = 1$ and [HaJ98a, Lemma 1.2] in the general case. Lemma 1.1.7 appears as [HaV96, Lemma 3.6].

The roles of P_i and Q_i in the patching data of [HaV96], [HaJ98a], etc. have been exchanged in this book in order for the smaller fields to be named by earlier letters.