

The proof of Theorem 4.10.3(a) uses the fact that $H = \text{Gal}(\mathbb{E}/\mathbb{B}_H)$, but the proof of this fact was omitted. Thus we need the following:

Theorem. *Let \mathbb{E} be a finite Galois extension of \mathbb{F} and let H be a subgroup of $\text{Gal}(\mathbb{E}/\mathbb{F})$. Let $\mathbb{B} = \text{Fix}(H)$. Then $H = \text{Gal}(\mathbb{E}/\mathbb{B})$.*

Proof. Since H fixes \mathbb{B} , we have that $H \subseteq \text{Gal}(\mathbb{E}/\mathbb{B})$. In order to show equality, we need only show that $|H| = |\text{Gal}(\mathbb{E}/\mathbb{B})|$. Let $n = |H|$ and $d = |\text{Gal}(\mathbb{E}/\mathbb{B})|$. Certainly $n \leq d$ so in order to show that $n = d$ we need only show that $d \leq n$. Since \mathbb{E} is a Galois extension of \mathbb{B} we know that $d = |\mathbb{E}/\mathbb{B}|$.

Proof. (Artin) We prove that $d \leq n$ by contradiction. Suppose that $d > n$.

Let $\{\varepsilon_1, \dots, \varepsilon_d\}$ be a basis for \mathbb{E} as a vector space over \mathbb{B} . Let $H = \{\sigma_1, \dots, \sigma_n\}$. Label these group elements so that σ_1 is the identity. Consider the system of linear equations

$$(\star_i) \quad \sigma_i(\varepsilon_1)x_1 + \dots + \sigma_d(\varepsilon_d)x_d = 0$$

for $i = 1, \dots, n$. This is a homogeneous linear system of n equations in d unknowns with $d > n$, so has a nontrivial solution. Choose a solution with the fewest number s of the x_i 's nonzero. Renumber if necessary so that these are $x_1 = \alpha_1, \dots, x_s = \alpha_s$. Note $s > 1$ as if $s = 1$, equation (\star_1) would give $\sigma_1(\varepsilon_1)\alpha_1 = 0$, i.e., $\varepsilon_1\alpha_1 = 0$, and hence $\varepsilon_1 = 0$; contradiction. Multiplying the α_i 's by α_s^{-1} if necessary, we may assume that $\alpha_s = 1$. Not all of the α_i 's can be in \mathbb{B} as if they were, equation (\star_1) would give $\sigma_1(\varepsilon_1)\alpha_1 + \dots + \sigma_1(\varepsilon_s)\alpha_s = 0$, i.e., $\varepsilon_1\alpha_1 + \dots + \varepsilon_s\alpha_s = 0$, contradicting the \mathbb{B} -linear independence of $\{\varepsilon_1, \dots, \varepsilon_n\}$. Thus some $\alpha_i \notin \mathbb{B}$. Renumber if necessary so that $\alpha_1 \notin \mathbb{B}$. Then equation (\star_i) gives

$$(\ast_i) \quad \sigma_i(\varepsilon_1)\alpha_1 + \dots + \sigma_i(\varepsilon_{s-1})\alpha_{s-1} + \sigma_i(\varepsilon_s) = 0$$

Since $\alpha_1 \notin \mathbb{B}$ and $\text{Fix}(H) = \mathbb{B}$, there is some $\sigma_k \in H$ with $\sigma_k(\alpha_1) \neq \alpha_1$. Since H is a group, for any $\sigma_i \in H$ there is a $\sigma_j \in H$ with $\sigma_i = \sigma_k\sigma_j$. Applying σ_k to equation (\ast_j) we obtain the equation

$$(\ast\ast_i) \quad \sigma_i(\varepsilon_1)\sigma_k(\alpha_1) + \dots + \sigma_i(\varepsilon_{s-1})\sigma_k(\alpha_{s-1}) + \sigma_i(\varepsilon_s) = 0$$

Then $(\ast_i) - (\ast\ast_i)$ is the equation

$$(\ast\ast\ast_i) \quad \sigma_i(\varepsilon_1)(\alpha_1 - \sigma_k(\alpha_1)) + \dots + \sigma_i(\varepsilon_{s-1})(\alpha_{s-1} - \sigma_k(\alpha_{s-1})) = 0$$

and this is true for $i = 1, \dots, n$. Let $x_i = \alpha_i - \sigma_k(\alpha_i)$ for $i = 1, \dots, s-1$ and $x_i = 0$ for $i = s, \dots, d$. Then $x_1 \neq 0$ as $\sigma_k(\alpha_1) \neq \alpha_1$, so this is a nontrivial solution to the system (\star_i) for $i = 1, \dots, n$ with fewer than s of the x_i 's nonzero; contradiction. \square

With this Theorem in hand, we can now simplify the proof that Γ is 1-1 as follows: Let H_1 and H_2 be subgroups of G . Suppose that $\mathbb{B}_{H_1} = \mathbb{B}_{H_2}$. Then

$$H_1 = \text{Gal}(\mathbb{B}_{H_1}) = \text{Gal}(\mathbb{B}_{H_2}) = H_2.$$

The rest of the proof of Theorem 4.10.3 is unchanged.