The main theorem of the Galois theory proven with ideas from the first *Mémoire* of Galois.

Math Dicker, Hoensbroek, the Netherlands

May 6, 2019

Abstract

A proof of the main theorem of the Galois theory is presented using the main theorem of symmetric polynomials. The idea originated from studying the *Mémoire sur les conditions de résolubilité des équations par radicaux* of Galois. The motto "Read the masters" pays off.

Introduction.

The Galois theory today is based on automorphisms of a field extension that leave the basic field invariant. Central in this theory is the well-known correspondence theorem usually proven with an Artin-Dedekind lemma. This article will provide a proof of this theorem which is inspired by ideas you can find in the *Mémoire sur les conditions de résolubilité des équations par radicaux*. For translations see [1, 2, 4], for the original manuscript see [3]. The article also refers to the main theorem of the symmetric polynomials which Galois also often uses. This article therefore shows that the motto "Read the masters" works.

The idea originates as follows: if you look at the $n \times m$ array below in proposition I of the *Mémoire* you see that $\phi V, \phi_1 V, \phi_2 V, ..., \phi_{m-1} V$, the roots of the given equation, are listed in different orders in $n$ rows. One entry of the $m$ roots in a row is called an arrangement of the roots $a, b, c, d, ...$. The $n$ arrangements form a so-called arrangement group and the corresponding substitution group is the Galois group of $F \subset F[a, b, c, d, ...]$ working on $a, b, c, d, ...$. For explanation: an arrangement group is a set of arrangements such that if $\alpha, \beta, \gamma \in G$ and $\phi_{\alpha, \beta}$ is the substitution (a bijection on $a, b, c, d, ...$) that transforms $\alpha$ to $\beta$ then $\phi_{\alpha, \beta}$ working on $\gamma$ is also $\in G$. If $G$ is an arrangement group you can make $\Pi(G) = \{\phi_{\alpha, \beta} | \alpha, \beta \in G\}$, the substitution group of $G$. This is a group in the modern sense. On the left of the $n \times m$ array are the corresponding values from Lemma II; important is that these are all different values. The values $V, V', V''$ ... are all primitive elements for the field $F[a, b, c, d, ...]$, this is lemma III. You can make the arrangements in the rows of the $n \times m$ array as follows; let

---

1Edwards and Tignol support this motto.
2For an excellent explanation of the concepts arrangement, arrangement group, substitution and substitution group see [6].
every automorphism of the Galois group transform \( V \) from Lemma II. If \( H \) is a subgroup of the Galois group we will add a field to \( H \) using an arrangement-group. The idea is this: let \( H \) be a subgroup of order \( k \) of the Galois group with \( H = \{ h_1, h_2, \ldots, h_k \} \), choose a random arrangement from the \( n \) rows and let \( \alpha \) be the corresponding primitive element on the left. We add to \( H \) the field \( \{ P(h_1(\alpha), h_2(\alpha), \ldots, h_k(\alpha)) | \ P \text{ a symmetric polynomial} \in F[x_1, x_2, \ldots, x_k] \} \). This field appears to be independent of the choice of the arrangement. If you let \( H \) operate on the chosen arrangement this will result in an arrangement-group with the same corresponding primitive elements. If you have an arrangement-group you can make the substitution-group; in this case you get \( H \). But this mapping is not injective; if you read the example before proposition VI where Galois shows that the roots of the quartic are radical, the arrangement-group of 12 arrangements is partitioned in 3 arrangement-groups of 4 elements. The substitution-groups of these 3 arrangement-groups are all the four-group of Klein. In case of a fixed arrangement \( \epsilon \) then you can prove that there is a one-to-one correspondence between the arrangement-groups containing \( \epsilon \) and the subfields of the splitting field mentioned above. We will start from a subgroup of automorphisms in the Galois group and prove the main theorem of the Galois theory in a modern way. The story above is only to illustrate that is very useful to study the original writings of Galois. I am also convinced that Galois knows everything about symmetric polynomials\(^3\) Galois gives in proposition I a characterization of \( F \) that refers strongly to the main theorem of Galois theory. We will prove this proposition at the end.

---

\(^3\)Read the very interesting article \[5\]
The proof.
A Galois extension can be seen as a splitting field over a basic field $F$ of a polynomial $\in F[x]$ with different roots. We assume that the integers form part of that basic field $F$ in connection with lemma II of Galois. Let $R=\{r_1, r_2, ..., r_n\}$ be the different roots of the aforementioned polynomial then $F \subset F[r_1, r_2, ..., r_n]$ is a Galois extension. Lemma’s II and III of Galois guarantee that there are primitive elements. Choose a primitive element $\omega$ for the Galois extension of $F \subset F[R]$. We define a mapping which to every subgroup in the Galois group of $F \subset F[R]$ assigns a field in $F[R]$; we prove that this mapping is surjective and injective. We also prove that this field is exactly the field referred to in the main theorem proven by E. Artin. Proposition I of in the Mémento is thereby proven.

We prove the main theorem of the Galois theory using the main theorem of the symmetric polynomials as you will see.

The definition af the field $L_{H,\omega}$.

[0] Let $H$ be a group and $H \subset \text{Galois group of } F \subset F[R]$; assume $H = \{\sigma_1, \sigma_2, ..., \sigma_m\}$ and $\sigma_i$ an automorphism of $F[R]$. Assign to $H$ the field $L_{H,\omega} = \{P(\sigma_1(\omega), \sigma_2(\omega), ..., \sigma_m(\omega)) | P \text{ a symmetric polynomial } \in F[x_1, x_2, ..., x_m]\}; F \subset L_{H,\omega}$ because if $x \in F$ use $P(x_1, x_2, ..., x_m) = x$. If $x \not\in F$ and $x$ in $L_{H,\omega}$ use the minimum polynomial of $x$ over $F$ to prove that $\frac{1}{x} \in L_{H,\omega}$.

Independence of the choice of the primitive element.

[1]: If $\theta$ is an other primitive element then $L_{H,\theta} = L_{H,\omega}$; $\theta = g(\omega)$ for some $g \in F[x]$; Substituting $\theta = g(\omega)$ implies $L_{H,\theta} \subset L_{H,\omega}$. The other inclusion mutatis mutandis.

Surjectivity. [2]: If $L$ is a subfield of $F[R]$ and $g$ is the minimal polynomial of $\omega$ over $L$ we consider the field $L_{G,\omega}$ with $G$ the Galois group of $L \subset F[R]$. Let $G = \{\tau_1, \tau_2, ..., \tau_n\}$ with $n$ equal to the degree of the extension $L \subset F[R]$. The polynomial $g(x) = \prod_{i=1}^{n} (x - \tau_i(\omega))$ is in $L[x]$ and in $L_{G,\omega}[x]$. Using the main theorem of symmetric polynomials and the coefficients of $g \in L[x]$ we know that $L_{G,\omega} \subset L$. The minimal polynomial of $\omega$ over $L_{G,\omega}$ divides $g$ and so $[F[R]:L_{G,\omega}] \leq [F[R]:L]$. Therefore also $L_{G,\omega} = L$ and the surjectivity is proven.

Injectivity. [3]: [2] has been proven for every subfield of $F[R]$, we apply [2] on $L=L_{H,\omega}$ with $H$ as in [0]. We are going to use the equality $L_{H,\omega} = L_{G,\omega}$ with $G$ as in [2]. Every automorphism $\in H$ is the identity on $L=L_{H,\omega}$, so $H \subset G$, the Galois group of $L=L_{G,\omega} \subset F[R]$. Therefore $m \leq n$. Let $f(x) = \prod_{i=1}^{m} (x - \sigma_i(\omega))$ then $f \in L[x] = L_{H,\omega}[x]$; the minimal polynomial $g$ of $\omega$ over $L=L_{G,\omega}$ in $L[x]$ has degree $n$ and divides $f$; consequently $n \leq m$ and so $n=m$ and $H=G$. The injectivity is proven; the assumption $H_1 \neq H_2$ and $L_{H_1,\omega} = L_{H_2,\omega}$ leads to a contradiction because then $H_1=H_2$ the Galois group of $(L_{H_1,\omega} = L_{H_2,\omega}) \subset F[R]$.

The main theorem of the Galois theory follows: the mapping which to a subgroup $H$ of the Galois group of $F \subset F[R]$ assigns the field $L_{H,\omega}$ is a one-to-one correspondence between the subgroups in the Ga-
lois group of $F \subset F[R]$ and the subfields in $F[R]$. $[F[R]:L_{H,\omega}]=|H|$ with $H$ the Galois group of $L_{H,\omega} \subset F[R]$.

Yet to prove $L_{H,\omega}=L^H$ where $L^H=\{x|\sigma(x)=x\text{ for all } \sigma \in H\}$. Let $x \in L^H$; there exists a polynomial $h$ in $F[x]$ with $x=h(\omega)$ and so $x=h(\sigma_i(x))=h(\sigma_i(\omega))$. Consider the symmetric polynomial $P(x_1,x_2,...,x_m)=(x_1+x_2+...+x_m)/m$; $x=P(x,x,...,x)=(h(\sigma_1(\omega))+h(\sigma_2(\omega))+...+h(\sigma_m(\omega)))/m$ and consequently $x \in L_{H,\omega}$. That $L_{H,\omega} \subset L^H$ is evident. This proves Proposition I in the *Mémoire* of Galois.

My email address is louis.dicker@ziggo.nl

**References**

[1] Harold M. Edwards, *Galois Theory*, Springer, 1984.

[2] Peter M. Neumann, *The mathematical writings of Évariste Galois*, European Mathematical Society, Zürich, 2011.

[3] For the original manuscript see http://bibliotheque-institutdefrance.fr

[4] Harold M. Edwards *Galois for 21st-century readers*. Notices Amer. Math. Soc., 59(7):912-923.

[5] Ben Blum-Smith and Samuel Coskey https://arxiv.org/abs/1301.7116

[6] Jean-Pierre Tignol, *Galois’ Theory of Algebraic Equations*, second edition, World Scientific, 2016.