I.G. Automorphisms and fixed fields

Begin with a field $L$ and its group $\text{Aut}(L)$ of automorphisms. To each subfield $K \subset L$ we can associate the subgroup

$$\text{Aut}(L/K) := \{\sigma \in \text{Aut}(L) \mid \sigma(k) = k \, (\forall k \in K)\} \leq \text{Aut}(L)$$

of automorphisms over $K$, which we will denote sometimes by the shorthand notation “$\Gamma(K)$”. Similarly, to each subgroup (or even subset) $G \leq \text{Aut}(L)$ we may associate the subfield

$$\text{Inv}(G) := \{\ell \in L \mid \sigma(\ell) = \ell \, (\forall g \in G)\} \subseteq L$$

of elements invariant under $G$, or “$\Phi(G)$” for short.\(^{21}\)

One notices immediately that both of these operations are \textit{contravariant} in the sense of reversing inclusions:

\[\begin{align*}
G_1 \supseteq G_2 \implies \text{Inv}(G_1) \subseteq \text{Inv}(G_2) \\
K_1 \supseteq K_2 \implies \text{Aut}(L/K_1) \subseteq \text{Aut}(L/K_2)
\end{align*}\]

That is, a larger set of automorphisms leaves a smaller field invariant, and a larger subfield has a smaller group of automorphisms fixing it. Yes, that’s nice, but how are the two operations \textit{related}?

I know what you really want to hear is “they produce a bijection between subfields of $L$ and subgroups of $\text{Aut}(L)$, and are inverse to each other.” We will eventually reach such a statement, but you will have to settle for a weaker, preliminary result at this stage:

**I.G.2. Proposition.** Let $A \subseteq \text{Aut}(L)$ be a subset, $\langle A \rangle$ the subgroup it generates, and $K \subset L$ a subfield. Then:

(i) $\Gamma \Phi(A) \supseteq A$.

(ii) $\Phi \Gamma(K) \supseteq K$.

(iii) $\Phi \Gamma \Phi(A) = \Phi(A)$.

(iv) $\Gamma \Phi \Gamma(K) = \Gamma(K)$.

(v) $\Phi(\langle A \rangle) = \Phi(A)$.

We can read (i) as saying that $A$ is among the automorphisms fixing its fixed field (though there may be more), and (ii) as saying that

\[^{21}\text{This is also called the “fixed field” of } G, \text{ hence the “} \Phi \text{“.}\]
$K$ is invariant by the automorphisms fixing it (though they may fix a larger subfield). Even better, (iii) and (iv) suggest that on subfields arising as fixed fields, and subgroups arising as “Galois groups,” we do get something like a bijection. On the other hand, (v) asserts that, if we don’t restrict at least to subgroups, we definitely don’t get a bijection.

**Proof.** (i) and (ii) are clear (see the above paragraph). For (iii), take $K = \Phi(A)$ and apply (ii) to get “$\supset$”; and apply $\Phi$ to (i) (and use (I.G.1)) to get “$\subseteq$”. For (iv), use a symmetric argument.

Finally, by (i), $\Gamma \Phi(A)$ is a group containing $A$, hence contains $\langle A \rangle$ (the minimal such group). Applying $\Phi$ (and (I.G.1) and (iii)) to $A \subset \langle A \rangle \subset \Gamma \Phi(A)$ gives $\Phi(A) \supset \Phi(\langle A \rangle) \supset \Phi \Gamma \Phi(A) = \Phi(A)$, hence the equality in (v).

Now given a subgroup $G = \{\sigma_1, \ldots, \sigma_{|G|}\} \leq \text{Aut}(L)$ and an element $\lambda \in L$, consider the orbit vector

$$\lambda^G := (\sigma_1(\lambda), \ldots, \sigma_{|G|}(\lambda)) \in L^{|G|},$$

where by $L^{|G|}$ we simply mean the $L$-vector space of dimension $|G|$.

**I.G.3. Lemma.** Set $K := \text{Inv}(G)$, and let $\Lambda \subset L$ be a subset. Then the following are equivalent:

(a) $\Lambda$ is linearly independent over $K$.
(b) $\{\lambda^G\}_{\lambda \in \Lambda}$ is linearly independent over $K$.
(c) $\{\lambda^G\}_{\lambda \in \Lambda}$ is linearly independent over $L$.

**Proof.** (c) $\implies$ (b): This is obvious.

(b) $\implies$ (a): If (a) fails, there exist $\lambda_1, \ldots, \lambda_r \in \Lambda$ such that $\sum_{i=1}^r k_i \lambda_i = 0$ with all $k_i \in K^*$. Since $K$ is fixed by $G$, $\sum_{i=1}^r k_i \sigma_j(\lambda_i) = 0$ for each $\sigma_j \in G$. Thus $\sum_{i=1}^r k_i \lambda_i^G = 0$ and (b) fails.

(a) $\implies$ (c): If (c) fails, let $\sum_{i=1}^r \ell_i \lambda_i^G = 0$ be a nontrivial relation ($\lambda_i \in \Lambda$, $\ell_i \in L^*$) with minimal $r (> 1)$. That is, for each $\sigma \in G$, we have

---

22 in [Jacobson]’s more general sense
\[\sum_{i=1}^r \ell_i \sigma(\lambda_i) = 0.\] Fixing any \(g \in G\), we replace \(\sigma\) by \(g^{-1}\sigma\) and apply \(g\) to get \(\sum_{i=1}^r g(\ell_i)\sigma(\lambda_i) = 0\), so that

\[
0 = \ell_r \sum_{i=1}^r g(\ell_i)\sigma(\lambda_i) - g(\ell_r) \sum_{i=1}^r \ell_i \sigma(\lambda_i) = \sum_{i=1}^{r-1} (g(\ell_i)\ell_r - g(\ell_r)\ell_i)\sigma(\lambda_i).
\]

By minimality of \(r\), each coefficient in the last sum must be 0: so \(g(\ell_i)\ell_r = g(\ell_r)\ell_i \implies g(\ell_i/\ell_r) = \ell_i/\ell_r\). Since \(g\) was arbitrary, \(\ell_i/\ell_r \in \text{Inv}(G) = K\). The \(\sigma = \text{id}\) component of \(\sum_{i=1}^r \frac{\ell_i}{\ell_r} \lambda_i^G = 0\) now reads \(\sum_{i=1}^r \frac{\ell_i}{\ell_r} \lambda_i = 0\), so that (a) fails. \(\square\)

From this Lemma we now deduce our first big advance towards the Galois correspondence:

I.G.4. THEOREM. Assume \(G \leq \text{Aut}(L)\) is finite. Then \(L/\text{Inv}(G)\) is Galois, \(G = \text{Aut}(L/\text{Inv}(G)) (= \Gamma\Phi(G))\), and \(|G| = [L: \text{Inv}(G)]\).

PROOF. Let \(K = \text{Inv}(G)\).

Let \(\Lambda \subset L\) be a subset which is linearly independent over \(K\); in particular, we may take \(|\Lambda| = [L:K]\). By the Lemma, the orbit vectors \(\{\lambda^G\}_{\lambda \in \Lambda} \subset L[G]\) are linearly independent over \(L\). Since \(\dim_L(L[G]) = |G|\), we must have \(|\Lambda| \leq |G|\) hence \([L:K] \leq |G|\).

On the other hand, by I.G.2(i) \(G \leq \text{Aut}(L/K)\), and by I.F.21 \(|\text{Aut}(L/K)| \leq [L:K]\) hence \(|G| \leq [L:K]\). Conclude that \(|G| = [L:K]\), forcing \(G = \text{Aut}(L/K)\), and by I.F.21 again, that \(L/K\) is Galois. \(\square\)

Suppose now we are given any field extension \(L/K\). The following is then immediate from I.G.4:

I.G.5. COROLLARY. Let \(G \leq \text{Aut}(L/K)\) be a finite subgroup, and put \(M := \text{Inv}(G)\). Then \(L/M\) is finite and normal (and separable).

(Of course, \(M/K\) could still be a mess — in particular, non-normal.)

In contrast to the last Theorem and Corollary, if we start with a subfield instead of a subgroup, we arrive at the following:

I.G.6. PROPOSITION. Let \(K \subset L\) be a subfield with \([L:K]\) finite, and put \(G := \text{Aut}(L/K)\). Then \(L/K\) is Galois \iff \(K = \text{Inv}(G)\) (\iff \(|G| = [L:K]\)). Otherwise, \(K \not\subset \text{Inv}(G)\) (\and \(|G| < [L:K]\)).
PROOF. The statements about $|G|$ and $[L:K]$ are from I.F.21; in particular, $|G| < \infty$. So I.G.4 applies, and $|G| = [L:\operatorname{Inv}(G)]$. Also, we know that $K \subseteq \operatorname{Inv}(G)$ from I.G.2(ii).

So if $L/K$ is Galois, then $|G| = [L:K] \implies [L:\operatorname{Inv}(G)] = [L:K]$ forces $\operatorname{Inv}(G) = K$. If $L/K$ is not Galois, then $|G| < [L:K] \implies [L:\operatorname{Inv}(G)] < [L:K] \implies [\operatorname{Inv}(G):K] > 1 \implies \operatorname{Inv}(G) \supseteq K$. $\square$

Here are some examples from [Jacobson]:

I.G.7. EXAMPLE. Assuming $\text{char}(K) \neq 2$, and that $a \in K$ has no square root in $K$, we consider the quadratic extension $L := K[x]/(x^2 - a)$. Writing $u$ for the image of $x$, sending $u \mapsto -u$ induces a nontrivial automorphism of $L/K$, namely $\sigma(k_1 + k_2u) := k_1 - k_2u$. Between this and $\text{id}_L$, we can’t have any more, since $|\operatorname{Aut}(L/K)| \leq [L:K] = 2$. (To see there are two, you could also use the fact that $L/K$ is a splitting field hence Galois.) So $\operatorname{Aut}(L/K) \cong \mathbb{Z}_2$.

I.G.8. EXAMPLE. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since this is a splitting field for $(x^2 - 2)(x^2 - 3)$ (hence Galois), and has degree $[L:K] = 4$, we must have $|\operatorname{Aut}(L/K)| = 4$. Alternatively, you can construct the 4 automorphisms and deduce $L/K$ is Galois from that. In fact, $\operatorname{Aut}(L/K)$ is the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$, with $\sigma(m,n)$ sending $\sqrt{2} \mapsto (-1)^m\sqrt{2}$ and $\sqrt{3} \mapsto (-1)^n\sqrt{3}$.

I.G.9. EXAMPLE. Consider an imperfect field $K$ of characteristic $p$, and $\alpha \in K \setminus \phi(K)$. Then $f(x) := x^p - \alpha$ is irreducible and inseparable, becoming (by I.E.9) a $p$th power $(x - u)^p$ in a splitting field $L = K(u) := K[x]/(f(x))$. Since an automorphism of $L/K$ must send any root of $f$ to another root, it sends $u \mapsto u$ hence is the identity. So $\operatorname{Aut}(L/K) = \{\text{id}_L\}$ is trivial, which also implies $L/K$ is not Galois, but we already knew that.

I.G.10. EXAMPLE. For a transcendental extension, look at $L = K(t)$, the rational function field in the indeterminate $t$. Any automorphism must send $t$ to another generator $u = f(t)/g(t)$ of $L$ (where

\footnote{Or you can just invoke the general result I.C.21(i).}
$f, g \in K[t]$ are coprime). Since $F(t) := f(t) - ug(t)$ is irreducible over $K[u]$ hence (by Gauss) $K(u), K(t) = K(u)[t]/(F(t))$ has degree $d := \max(\deg(f), \deg(g))$ over $K(u)$, which means $u$ is a generator (i.e. $K(u) = K(t)$) iff $d = 1$. Conclude that $u = (at + b)/(ct + d)$, with $ad - bc \neq 0$ so that $f$ and $g$ are indeed coprime.

In other words, the automorphisms are pullback maps along “fractional linear transformations”, and we have $\text{Aut}(L/K) \cong \text{PSL}_2(K)$: to each $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PSL}_2(K)$, we associate $\sigma_M$ sending $t \mapsto \sigma_M(t) := \frac{at + b}{ct + d}$, and then any rational expression $R(t) \in L$ has $\sigma_M(R(t)) = R(\sigma_M(t))$. 