WIKIPEDIA

Galois group

In mathematics, more specifically in the area of abstract algebra known as Galois theory, the **Galois group** of a certain type of field extension is a specific group associated with the field extension. The study of field extensions and their relationship to the polynomials that give rise to them via Galois groups is called Galois theory, so named in honor of Évariste Galois who first discovered them.

For a more elementary discussion of Galois groups in terms of permutation groups, see the article on Galois theory.

Contents

Definition

Suppose that E is an extension of the field F (written as E/F and read "E over F"). An automorphism of E/F is defined to be an automorphism of E that fixes F pointwise. In other words, an automorphism of E/F is an isomorphism α from E to E such that $\alpha(x) = x$ for each $x \in F$. The set of all automorphisms of E/F forms a group with the operation of function composition. This group is sometimes denoted by $\operatorname{Aut}(E/F)$.

If E/F is a Galois extension, then $\operatorname{Aut}(E/F)$ is called the "Galois group of (the extension) E over F, and is usually denoted by $\operatorname{Gal}(E/F)$.[1]

If E/F is not a Galois extension, then the Galois group of (the extension) E over F is sometimes defined as $\operatorname{Aut}(G/F)$, where G is the Galois closure of E.

Examples

In the following examples F is a field, and $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$ are the fields of complex, real, and rational numbers, respectively. The notation $F(a)$ indicates the field extension obtained by adjoining an element a to the field F.

- $\operatorname{Gal}(F/F)$ is the trivial group that has a single element, namely the identity automorphism.
- $\operatorname{Gal}(\mathbf{C}/\mathbf{R})$ has two elements, the identity automorphism and the complex conjugation automorphism.[2]
- $\operatorname{Aut}(\mathbf{R}/\mathbf{Q})$ is trivial. Indeed, it can be shown that any automorphism of $\mathbf{R}$ must preserve the ordering of the real numbers and hence must be the identity.
- $\operatorname{Aut}(\mathbf{C}/\mathbf{Q})$ is an infinite group.
- $\operatorname{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ has two elements, the identity automorphism and the automorphism which exchanges $\sqrt{2}$ and $-\sqrt{2}$.
- Consider the field $K = \mathbf{Q}(\sqrt[3]{2})$. The group $\operatorname{Aut}(K/\mathbf{Q})$ contains only the identity automorphism. This is because K is not a normal extension, since the other two complex cube roots of 2 are missing from the extension—in other words K is not a splitting field.

- Consider now $L = \mathbf{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity. The group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to S_3, the dihedral group of order 6, and L is in fact the splitting field of $x^3 - 2$ over $\mathbf{Q}$.
- If q is a prime power, and if $F = \mathbf{GF}(q)$ and $E = \mathbf{GF}(q^n)$ denote the Galois fields of order q and q^n respectively, then $\mathrm{Gal}(E/F)$ is cyclic of order n and generated by the Frobenius homomorphism.
- If f is an irreducible polynomial of prime degree p with rational coefficients and exactly two non-real roots, then the Galois group of f is the full symmetric group S_p.

Properties

The significance of an extension being Galois is that it obeys the fundamental theorem of Galois theory: the closed (with respect to the Krull topology) subgroups of the Galois group correspond to the intermediate fields of the field extension.

If E/F is a Galois extension, then $\mathrm{Gal}(E/F)$ can be given a topology, called the Krull topology, that makes it into a profinite group.

See also

- Absolute Galois group

Notes

1. Some authors refer to $\mathrm{Aut}(E/F)$ as the Galois group for arbitrary extensions E/F and use the corresponding notation, e.g. Jacobson 2009.
2. Cooke, Roger L. (2008), *Classical Algebra: Its Nature, Origins, and Uses* (https://books.google.com/books?id=JG-skeT1eWAC&pg=PA138), John Wiley & Sons, p. 138, ISBN 9780470277973.

References

- Jacobson, Nathan (2009) [1985]. *Basic Algebra I* (2nd ed.). Dover Publications. ISBN 978-0-486-47189-1.
- Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556

External links

- Hazewinkel, Michiel, ed. (2001) [1994], "Galois group", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- "Galois Groups". *MathPages.com*.