Ideas of Galois

Group of permutations of roots of a polynomial.

For example, $x^4 + px^2 + q = 0$

Roots:
$x_{1,2} = \pm\sqrt{\frac{-p+\sqrt{p^2-4q}}{2}}$ and
$x_{3,4} = \pm\sqrt{\frac{-p-\sqrt{p^2-4q}}{2}}$

Note: $x_1+x_2 = 0$, $x_3+x_4 = 0$, but $x_1+x_3 \neq 0$

Ideas of Galois

$x_1 + x_2 = 0$, $x_3 + x_4 = 0$, but $x_1 + x_3 \neq 0$

Consider $R = \mathbb{Q}(p, q)$, the set of all rational functions of variables p, q with coefficients in $\mathbb{Q}$. This includes $\frac{3p^2-4q}{q^2-7p}$ and similar.

Some permutations preserve the root relations - 8 of the 24. These 8 are the *group of the equation in* R.

Notice: $x_1^2 - x_3^2 = \sqrt{p^2 - 4q}$. Add this to R, so $R' = R\left(\sqrt{p^2 - 4q}\right)$.

New relation in R' so *group of the equation in* R' is smaller, now only 4 permutations.

Continue: expand field and narrow group . . . until group only has one element.

Ideas of Galois

Galois considered an equation and found this sequence of groups - **without knowing the roots**.

He then asked which expressions are unrelated at one level, but are related at the next, e.g. $x_1^2 - x_3^2$. He called these *resolvents*. If they subgroups of the permutations are related in certain ways (minimal normal subgroups), then the equations can be solved by radicals. If the subgroups are index 2, then the roots are constructible using compass and straightedge.