Galois
- Born 1811
- Published at age 18
- Cursed out examiner at École Polytechnique (denied entry)
- Expelled from École Normale for political editorial
- Joined a Republican artillery unit of the National Guard that was then disbanded for plotting a coup.
- Imprisoned for six months after political protest
- Killed in a duel. Final words to his younger brother: "Don't cry, Alfred! I need all my courage to die at twenty!"
- Mathematical testament written night before death outlined his work. "Ask Jacobi or Gauss to publicly give their opinion, not as to the truth, but as to the importance of these theorems. Later, there will be, I hope, some people who will find it to their advantage to decipher all this mess." Indeed — us!

Main idea Translate properties of algebraic solutions to polynomial equations into properties of the Galois group of automorphisms of the splitting field.

2.1 Polynomials of several variables

Variables $x_1, x_2, \dots, x_n$

For F a field, $F[x_1, \dots, x_n] = \{$polynomials in $x_1, \dots, x_n$ with coefficients in $F\}$

Monomial: $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, $a_i \in \mathbb{N}$

Term: $c x_1^{a_1} \cdots x_n^{a_n}$, $c \in F$

Polynomial: sum of terms

The degree of a term $cx_1^{a_1}\cdots x_n^{a_n}$ is $a_1+\cdots+a_n$ $(c\neq 0)$.
The degree $\deg(f)$ of a polynomial f is the maximal degree of its terms $(f\neq 0)$. Define $\deg(0) = -\infty$.
Check $\deg(fg) = \deg(f)+\deg(g)$.
Think Pair Share: Why does this imply that $F[x_1,\dots,x_n]$ is an integral domain? (No zero divisors.)

Thm $F[x_1,\dots,x_n]$ is a unique factorization domain.
Rmk But for $n>1$, $F[x_1,\dots,x_n]$ is not a PID!
Thm F a field, R an F-algebra (commutative ring containing F). Then for any set function $f:\{x_1,\dots,x_n\}\longrightarrow R$ there is a unique ring homomorphism $g: F[x_1,\dots,x_n]\longrightarrow R$ such that $g(x_i) = f(x_i)$, $i=1,\dots,n$. I.e.

$$\begin{array}{ccc} \{x_1,\dots,x_n\} & \xrightarrow{f} & R \\ {\scriptstyle x_i}\downarrow & \nearrow_{\exists! g} & \\ x_i\ F[x_1,\dots,x_n] & & \end{array}$$

Rmk · g is evaluation at $f(x_1),\dots,f(x_n)$:

$$g: h(x_1,\dots,x_n)\longmapsto h(f(x_1),\dots,f(x_n))$$

· Say that $F[x_1,\dots,x_n]$ is the free F-algebra on $\{x_1,\dots,x_n\}$.

Defn $x_1,\dots,x_n$ variables over a field F. The elementary symmetric polynomials $\sigma_1,\dots,\sigma_n\in F[x_1,\dots,x_n]$ are

$$\sigma_1 := x_1+\cdots+x_n$$
$$\sigma_2 := \sum_{1\le i<j\le n} x_ix_j$$
$$\sigma_3 := \sum_{1\le i<j<k\le n} x_ix_jx_k$$
$$\vdots$$
$$\sigma_r := \sum_{1\le i_1<i_2<\cdots<i_r\le n} x_{i_1}x_{i_2}\cdots x_{i_r}$$
$$\vdots$$
$$\sigma_n := x_1x_2\cdots x_n$$

Prop $(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n$

i.e. $\prod_{i=1}^{n}(x-x_i) = \sum_{i=0}^{n}(-1)^i \sigma_i x^{n-i}$ where $\sigma_0 := 1$.

Pf When multiplying out $\prod_{i=1}^{n}(x-x_i)$, we get an x^{n-i} term when we take $n-i$ x's and i x_j's, each of which comes with a (-1) coefficient. Thus the coefficient of x^{n-i} is

$$\sum_{1 \le j_1 < j_2 < \cdots < j_i \le n} (-1)^i x_{j_1} x_{j_2} \cdots x_{j_i} = (-1)^i \sigma_i . \qquad \square$$

Cor If $f = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in F[x]$ has roots $\alpha_1, \ldots, \alpha_n \in L \supseteq F$, then $a_r = (-1)^r \sigma_r(\alpha_1, \ldots, \alpha_n)$. $\square$