Computing Galois Groups of irreducible quartic polynomials

Let char$K \neq 2$ and $f(X) \in K[X]$ be an irreducible, separable polynomial of degree 4, with $Z_f = \{\alpha_1, \ldots, \alpha_4\}$. By proposition 2 we know that its Galois group G_f is a transitive subgroup of S_4 divisible by 4, thus G_f could be S_4 of order 24, A_4 of order 12, $V \subset A_4$ of order 4, D_4 of order 8 (three of them in S_4) or C_4 of order 4 (three of them in S_4). We introduce a polynomial of degree 3 with all of its roots in K_f known as *the resolvent* $R_f(X)$ *of* f, which will help us determine if 3 divides the order of G_f.

The resolvent of $f(X)$.

We consider the elements of K_f, $\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4,\ \beta = \alpha_1\alpha_3 + \alpha_2\alpha_4,\ \gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$, and the cubic polynomial

$$R_f(X) = (X-\alpha)(X-\beta)(X-\gamma) \in K_f[X],$$

with $M = K[\alpha,\beta,\gamma] \subset K_f$, which satisfies $M = K_f^V$, and $\text{Disc}(f) = \text{Disc}(R_f)$, since

$$\alpha-\beta = (\alpha_1-\alpha_4)(\alpha_2-\alpha_3),\ \alpha-\gamma = (\alpha_1-\alpha_4)(\alpha_2-\alpha_3),\ \beta-\gamma = (\alpha_2-\alpha_1)(\alpha_4-\alpha_3).$$

To find the exact value of the resolvent $R_f[X]$ of f, we expand the product in the left of

$$f(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4) = X^4 + aX^3 + bX^2 + cX + d,$$

and we write the α_i's in terms of a, b, c and d, getting

$$R_f(X) = X^2 - bX^2 + (ac-4d)X - (a^2d + c^2 - 4bd).$$

(a) $R_f(X)$ irreducible in $K[X]$ if and only if 3 divides $|G_f|$.

(b) If $R_f(X)$ is irreducible, then $[M:K] = 3$ and 3 divides $[K_f:K] = |G_f|$. In this case, G_f is completely determined by Disc(f): $\text{Disc}(f) = \square \Rightarrow G_f = A_4$; $\text{Disc}(f) \neq \square \Rightarrow G_f = S_4$

(c) If $R_f(X)$ is reducible in $K[X]$, then there is no element of order 3 in G_f, so G_f is either V, D_4 or C_4.

(d) If all roots of $R_f(X)$ are in K, then $M = K$ and $G_f = V$. If only one root of R_f is in K, then $M = K[\sqrt{D}]$ and G_f is completely determined by whether $f(X)$ remains irreducible in $M[X]$.

Galois groups of irreducible, separable quartic polynomials if char$K \neq 2$

$R_f(X)$ in $K[X]$	D in K	M	f in M	G_f
irreducible	$\neq \square$			S_4
irreducible	$= \square$			A_4
reducible	$(= \square)$	K		V
reducible	$(\neq \square)$	$K[\sqrt{D}]$	irreducible	D_4
reducible	$(\neq \square)$	$K[\sqrt{D}]$	reducible	C_4

Examples in $\mathbb{Q}[X]$.

$f(X)$	$R_f(X)$	D	M	f in $\mathbb{Q}[\sqrt{D}]$	G_f
$X^4 - X - 1$	$X^3 - 4x - 1$	-283			S_4
$X^4 - 8X + 12$	$X^3 - 48X - 64$	576^2			A_4
$X^4 + 36X + 63$	$(X-18)(X+6)(X+12)$	4320^2	$\mathbb{Q}$		V
$X^4 + 5X^2 + 5$	$(X-5)(X^2-20)$		$\mathbb{Q}(\sqrt{5})$	$\left(X^2 + \frac{5+\sqrt{5}}{2}\right)\left(X^2 - \frac{5+\sqrt{5}}{2}\right)$	C_4

Construction of finite fields:

We review the following facts from Module 2 (Lecture 5) and Module 3 (Lectures 1 , 2)

(i) If K is a field, the characteristic of K, denoted by char$K$ is the smallest n such that $1 + \overset{n)}{\cdots} 1 = 0$. If char$K \neq 0$, then char$K$ is a prime number p.

(ii) Examples of fields with characteristic 0 are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Examples of fields with characteristic a prime p are $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_{p^r} = \mathbb{F}_[X]/(f)$, where $f(X)$ is a polinomial of degree r which is irreducible modulo p

Proposition 1

(a) The cardinality of a field K of characteristic p is $q = p^n$, some $n \geq 1$. Also, K contains $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(b) The additive group $(K, +)$ of a finite field K is isomorphic to $(\mathbb{Z}/p\mathbb{Z}, \overset{n)}{\ldots}, \mathbb{Z}/p\mathbb{Z})$

(c) The multiplicative group $(K^\times, \cdot)$ of a finite field K is cyclic

(d) There exists $\alpha \in K$ with $K = \mathbb{F}_p[\alpha]$.

(e) A finite field K is of the form $K = \mathbb{F}_p[X]/(f)$ where $f(X)$ is an irreducible polynomial (modulo p) of degree n.