The irreducibility of $x^{2p} - x^p + m^p$

Seminar Notes: 02/17/06

This talk is from joint work with Florian Luca, Pante Stănică, and Rob Underwood concerning the polynomials:

$$f_{p,m}(x) = 1 + \sum_{i=0}^{(p-1)/2} (-1)^i \frac{p}{p-i} \binom{p-i}{i} m^i x^{p-2i},$$

Theorem 1. *Let $p \geq 5$ be prime. Let K be the splitting field of $f_{p,1}(x)$ over $\mathbb{Q}$. Then the Galois group of $K/\mathbb{Q}$ is cyclic of order $p-1$.*

Theorem 2. *Let $p \geq 5$ be a prime, and let $m \geq 2$ be an integer. The Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$ is a subgroup of the symmetric group S_p of order $p(p-1)$ generated by a cycle of length p and a cycle of length $p-1$.*

Lemma. *Let p be an odd prime and let m be an integer with $m \geq 2$. Then the polynomial $x^{2p} - x^p + m^p$ is irreducible.*

Notation: $N = 1 - 4m^p$

$\gamma = (1+\sqrt{N})/2$, a root of $x^2 - x + m^p$

λ is a fixed p^{th} root of γ, a root of $x^{2p} - x^p + m^p$

$D < 0$ is a squarefree integer, $D|N$, and N/D is a square, so $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{D})$

Basic Steps of One Argument:

- For an irreducible $f(x) \in \mathbb{Q}[x]$ and a $g(x) \in \mathbb{Q}[x]$, the polynomial $f(g(x))$ is irreducible over $\mathbb{Q}$ if and only if $g(x) - \alpha$ is irreducible over $\mathbb{Q}(\alpha)$ where α is an arbitrary fixed root of $f(x)$.
- Take $f(x) = x^2 - x + m^p = (x-\gamma)(x-\overline{\gamma})$ and $g(x) = x^p$.
- The polynomial $x^p - \gamma$ is reducible in $\mathbb{Q}(\gamma)$ if and only if γ is a p^{th} power in $\mathbb{Q}(\gamma)$.
- Fix α and $\beta = \overline{\alpha}$ in $\mathbb{Q}(\sqrt{D})$ with
$$\alpha^p = \frac{1+\sqrt{1-4m^p}}{2} = \frac{1+\sqrt{N}}{2} \qquad \text{and} \qquad \beta^p = \frac{1-\sqrt{1-4m^p}}{2} = \frac{1-\sqrt{N}}{2}.$$
- Deduce $\alpha\beta = m$ and $\alpha + \beta = \pm 1$.
- Set $\alpha = (a+b\sqrt{D})/2$ and use that $2^{p-1} + 2^{p-1}\sqrt{N} = 2^p\alpha^p = (a+b\sqrt{D})^p = A + B\sqrt{D}$. Then $a^p \equiv 2^{p-1} \equiv 1 \pmod{p}$. Deduce $\alpha + \beta = +1$.
- The above implies α and β are both roots of $x^2 - x + m$.
- Write $\alpha = se^{i\theta}$ and $\beta = se^{-i\theta}$ where $s > 0$ and $\theta \in [0, 2\pi)$.
- From $s = \sqrt{m}$, $\cos\theta = 1/(2\sqrt{m})$ and $s^p\cos(p\theta) = \Re(\alpha^p) = 1/2$, deduce $\cos(p\theta) = 1/(2m^{p/2})$.
- Write $\cos(p\theta) = 2^{p-1}(\cos\theta)^p - 2^{p-3}p(\cos\theta)^{p-2} + \cdots$, where what remains on the right is a sum of smaller odd powers of $\cos\theta$ times p times rational integers and the coefficient of each term $(\cos\theta)^j$ on the right is divisible by 2^{j-1}. This can be seen by setting $w = e^{i\theta} + e^{-i\theta} = 2\cos\theta$ and considering $w^k = \sum_{j=0}^{k}\binom{k}{j}e^{(k-2j)i\theta}$ where k is odd; then express $2\cos(p\theta) = e^{ip\theta} + e^{-ip\theta}$ in terms of the w^k.
- Note $\cos(p\theta) = 2^{p-1}(\cos\theta)^p$, and deduce $(2\cos\theta)^2$ is a root of a monic $u(x) \in \mathbb{Z}[x]$ with $\deg u = (p-3)/2$.
- As $m \geq 2$, we have $(2\cos\theta)^2 = 1/m \notin \mathbb{Z}$, a contradiction.