Kris Harper
MATH 25900
May 14, 2010

Homework 5

Problem 1 (14.5.3). *Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5^{th} root of unity ζ_5. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicitly solve for the 5^{th} root of unity.*

Proof. Let $\zeta = \zeta_5$. Note that $\alpha^2 + \alpha - 1 = (\zeta + \zeta^{-1})^2 + \zeta + \zeta^{-1} - 1 = \zeta^2 + 2 + \zeta^{-2} + \zeta + \zeta^{-1} - 1 = \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$. Now note that $\zeta^2 - \alpha\zeta + 1 = \zeta^2 - \zeta^2 - 1 + 1 = 0$ so ζ satisfies $x^2 - \alpha x + 1$. Now note that $\alpha = (-1 \pm \sqrt{1+4})/2 = (-1 \pm \sqrt{5})/2$. Then

$$\zeta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} = \frac{1}{2}\left(\frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{\left(\frac{-1 \pm \sqrt{5}}{2}\right)^2 - 4}\right) = \frac{1}{4}\left(-1 \pm \sqrt{5} + i\sqrt{2(5 \pm \sqrt{5})}\right).$$

□

Problem 2 (14.5.4). *Let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the automorphism of the cyclotomic field of n^{th} roots of unity which maps ζ_n to ζ_n^a where a is relatively prime to n and ζ_n is a primitive n^{th} root of unity. Show that $\sigma_a(\zeta) = \zeta^a$ for* every *n^{th} root of unity.*

Proof. Let ζ be an n^{th} root of unity. Then we know $\zeta = \zeta_n^b$ for some integer b with $(b, n) = 1$. Now $\sigma_a(\zeta) = \sigma_a(\zeta_n^b) = \sigma(\zeta_n)^b = (\zeta_n^a)^b = (\zeta_n^b)^a = \zeta^a$. □

Problem 3 (14.5.6). *Let ζ_n denote a primitive n^{th} root of unity and let $K = \mathbb{Q}(\zeta_n)$ be the associated cyclotomic field. Let a denote the trace of ζ_n from K to $\mathbb{Q}$. Prove that $a = 1$ if $n = 1$, $a = 0$ if n is divisible by the square of a prime, and $a = (-1)^r$ if n is the product of r distinct primes.*

Proof. Note that a is simply the sum of the primitive n^{th} roots of unity. Let $f(n)$ be the sum of the primitive n^{th} roots of unity and let $g(n)$ be the sum of the n^{th} roots of unity. Note that $g(1) = 1$ and $g(0) = 0$ which can be seen by looking at the roots of unity in the complex plane and pairing them up on opposite sides of the real and imaginary axes. If we group the roots of unity by the divisors of n we see that $g(n) = \sum_{d|n} f(d)$. Then Möbius inversion tells us that $f(n) = \sum_{d|n} \mu(d) g(d/n) = \mu(n)$. □

Problem 4 (14.6.2). *Determine the Galois groups of the following polynomials:*
(a) $x^3 - x^2 - 4$ (b) $x^3 - 2x + 4$ (c) $x^3 - x + 1$ (d) $x^3 + x^2 - 2x - 1$.

Proof. (a) This factors as $(x - 2)(x^2 + x + 2)$ and the quadratic term is irreducible using the quadratic formula. The Galois group is thus of order 2.

(b) This factors as $(x+2)(x^2 - 2x + 2)$ and the quadratic term is irreducible using the quadratic formula. The Galois group is thus of order 2.

(c) This is irreducible using the rational root theorem since ± 1 are not roots. The discriminant $0^2(-1)^2 - 4(-1)^3 - 4(0)^3(1) - 27(1)^2 + 18(0)(-1)(1) = 4 - 27 = -23$ is not a square so the Galois group is S_3.

(d) This is irreducible using the rational root theorem since ± 1 are not roots. The discriminant $(1)^2(-2)^2 - 4(-2)^3 - 4(1)^3(-1) - 27(-1)^2 + 18(1)(-2)(-1) = 4 + 32 + 4 - 27 + 36 = 49$ is a square so the Galois group is A_3. □

Problem 5 (14.6.3). *Prove for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$.*

Proof. If $x^3 + ax + b$ is irreducible and degree 3 we know that its Galois group is either A_3 or S_3. But it's over a finite field so it must have cyclic Galois group, namely A_3. This means the discriminant is a square. The discriminant is $0^2a^2 - 4a^3 - 4(0)^3b - 27b^2 + 18(0)ab = -4a^3 - 27b^2$. □

Problem 6 (14.6.6). *Determine the Galois group of $x^4 + 3x^3 - 3x - 2$.*

Proof. Putting in ± 1 gives -1 and putting in ± 2 gives 32 and -4 so there is no linear factor by the rational root test. Suppose $x^4+3x^3-3x-2 = (x^2+bx+c)(x^2+ex+f) = x^4+(b+e)x^3+(c+f+be)x^2+(bf+ce)x+cf$. Then $b+e = 3$, $c+f+be = 0$, $bf+ce = -3$ and $cf = -2$. This means $c = \pm 1$ and $f = \mp 2$ so that $c+f = \pm 1 \mp 2 = \pm 1$ and $0 = c+f+be = \pm 1 + be$. Thus $be = \pm 1$ so $b = e = \pm 1$. But $b+e = 3$, a contradiction. Therefore x^4+3x^3-3x-2 is irreducible.

In this case $p = 1/8(-3(3)^2+8(0)) = -27/8$, $q = 1/8(3^3-4(3)(0)+8(-3)) = 3/8$ and $r = 1/256(-3(3)^4+16(3)^2(0)-64(3)(-3)+256(-2)) = -179/256$. This gives a resultant cubic of $h(x) = x^3+27/4x^2+227/16x+9/64 = 1/64(64x^3+432x^2+908x+9)$. Putting in ± 1, ± 3 and ± 9 gives 1413, -531, 8349, -555, 89829 and -19827 respectively so this is irreducible by the rational root test. Also $h(x)$ has discriminant $((27/4)^2(227/16)^2 - 4(227/16)^3 - 4(27/4)^3(9/64) - 27(9/64)^2 + 18(27/4)(227/16)(9/64) = -2183$ which is not a square. Thus this polynomial has Galois group S_4. $\square$

Problem 7 (14.6.7)**.** *Determine the Galois group of* x^4+2x^2+x+3.

Proof. Reducing modulo 2 gives x^4+x+1 which is irreducible over $\mathbb{F}_2$ thus also over $\mathbb{Q}$. Since there is no cubic term we easily compute that $p = 2$, $q = 1$ and $r = 3$ giving a resolvent cubic of $h(x) = x^3-4x^2-8x+1$. This is irreducible by the rational root test since ± 1 gives no zeros. The discriminant of $h(x)$ is $(-4)^2(-8)^2 - 4(-8)^3 - 4(-4)^3(1) - 27(1)^3 + 18(-4)(-8)(1) = 3877$ which is not a square. Thus the Galois group of this polynomial is S_4. $\square$

Problem 8 (14.6.8)**.** *Determine the Galois group of* $x^4+8x+12$.

Proof. Putting in the values ± 1, ± 2, ± 3, ± 4, ± 6 and 12 gives 21, 5, 44, 12, 117, 69, 300, 236, 1356, 1260, 20844 and 20652 so there is no linear factor by the rational root test. Suppose now $x^4+8x+12 = (x^2+bx+c)(x^2+ex+f) = x^4+(b+e)x^3+(c+f+be)x^2+(bf+ce)x+cf$ so that $b+e = c+f+be = 0$, $bf+ce = 8$ and $cf = 12$. Then $b = -e$ so $c+f = b^2$. Given that $cf = 12$, and they add to a nonnegative number, the possibilities for c and f are 1, 2, 3, 4, 6 and 12. But $1+12 = 13$, $2+6 = 8$ and $3+4 = 7$ none of which are square numbers. This is a contradiction, so $x^4+8x+12$ must be irreducible.

We easily see that $p = 0$, $q = 8$ and $r = 12$ giving a resultant cubic of $h(x) = x^3-48x+64$. Putting in ± 1, ± 2, ± 4, ± 8, ± 16, ± 32, ± 64 gives 17, 111, -24, 152, -64, 192, 192, -64, 3392, -3264, 31296, -31168, 259136 and -259008 showing that $h(x)$ is irreducible. The discriminant of $h(x)$ is $(0)^2(-48)^2 - 4(-48)^3 - 4(0)^3(64) - 27(64)^2 + 18(0)(-48)(64) = 331776 = 576^2$. Since $h(x)$ is irreducible and the discriminant is a square we see that the Galois group is A_4. $\square$

Problem 9 (14.6.11)**.** *Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4, A_4 or the dihedral group D_8 of order 8. Prove the the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.*

Proof. Since F is a degree 4 extension, it's generated by a root α of some fourth degree polynomial $p(x) \in \mathbb{Q}[x]$. But since F is not Galois, it's not a splitting field for $p(x)$ so in F we must have either $p(x) = (x-\alpha)q(x)$ or $(x-\alpha)(x-\beta)q(x)$ where $q(x)$ is either an irreducible cubic or an irreducible quadratic in $F[x]$. The Galois group is now determined by the extension of L/F where L is the galois closure of F, namely, the splitting field for $p(x)$. If $[L : F] = 6$ then $[L : \mathbb{Q}] = 24$ and the Galois group is S_4. If $[L : F] = 3$ then $[L : \mathbb{Q}] = 12$ and the Galois group is A_4. These cover all the possibilities for the first case since then $q(x)$ is an irreducible cubic over F so the extension must be 3 or 6. In the second case we must have $[L : F] = 2$ so $[L : \mathbb{Q}] = 8$ and D_8 is the Galois group.

Thus if F contains a quadratic extension of $\mathbb{Q}$ then $\mathbb{Q}(\sqrt{D}) \subseteq F$ for some squarefree element of $\mathbb{Q}$. But this implies $p(x) = (x \pm \sqrt{D})q(x)$ over F for a quadratic $q(x)$. Thus the Galois group must be D_8 as above. Conversely, if the Galois group is D_8, then $p(x)$ must split as $(x-\alpha)(x-\beta)q(x)$ over F. But since $\alpha, \beta \notin \mathbb{Q}$ this simplifies to saying that F contains a quadratic extension of $\mathbb{Q}$. $\square$

Problem 10 (14.6.13)**.** *(a) Let $\pm\alpha$, $\pm\beta$ denote the roots of the polynomial $f(x) = x^4+ax^2+b \in \mathbb{Z}[x]$. Prove that $f(x)$ is irreducible if and only if α^2, $\alpha \pm \beta$ are not elements of $\mathbb{Q}$.*

(b) Suppose $f(x)$ is irreducible and let G be the Galois group of $f(x)$. Prove that
(i) $G \cong V$, the Klein 4-group, if and only if b is a square in $\mathbb{Q}$ if and only if $\alpha\beta \in \mathbb{Q}$ is rational.
(ii) $G \cong C$, the cyclic group of order 4, if and only if $b(a^2-4b)$ is a square in $\mathbb{Q}$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.
(iii) $G \cong D_8$, the dihedral group of order 8, if and only if b and $b(a^2-4b)$ are not squares in $\mathbb{Q}$ if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

Proof. (a) Suppose that $\alpha^2, \alpha \pm \beta \notin \mathbb{Q}$. Then $\alpha = 1/2(\alpha+\beta+\alpha-\beta)$ and $\beta = 1/2(\alpha+\beta-(\alpha-\beta))$ are not in $\mathbb{Q}$ either. Thus $f(x)$ cannot factor as $(x-a')(x^3+b'x^2+c'x+d')$ because $a' \notin \mathbb{Q}$.

So suppose $x^4+ax^2+b = (x^2+cx+d)(x^2+ex+f) = x^4+(c+e)x^3+(d+f+ce)x^2+(cf+de)x+df$. This gives $c+e = cf+de = 0$ and $df = b$ so that $c = -e$ and $c(f-d) = 0$. Suppose first $c = 0$. The roots to x^2+cx+d are $(1/2)(-c \pm \sqrt{c^2-4d})$. Without loss of generality we can assume $\alpha = (1/2)(-c+\sqrt{c^2-4d})$ so that $\alpha^2 = (1/4)(c^2-2c\sqrt{c^2-4d}+c^2-4d)$. But if $c = 0$ this reduces to $-d$ showing that $-d \notin \mathbb{Q}$, a contradiction. On the other hand, suppose $f-d = 0$ so that $f = d$. Since $c = -e$ we can then express all four roots as $(1/2)(\pm c \pm \sqrt{c^2-4d})$. But then $\alpha - \beta = 0$, a contradiction. Therefore $f(x)$ doesn't split into a linear factor and a cubic or into two quadratics, so it must be irreducible.

Conversely, suppose $f(x)$ is irreducible. Then we know $\pm\alpha$ and $\pm\beta$ are not elements of $\mathbb{Q}$. Note that $x^4+ax^2+b = (x^2-(1/2)(-a+\sqrt{a^2-4b}))(x^2-(1/2)(-a-\sqrt{a^2-4b}))$. This gives the four solutions

$$\pm\sqrt{\frac{-a \pm \sqrt{a^2-4b}}{2}}.$$

Without loss of generality take α to be the solution with two $+$ signs. Then $\alpha^2 = (1/2)(-a+\sqrt{a^2-4b})$. Since $f(x)$ is irreducible and of degree 4 we know $a^2-4b \neq 0$ and squarefree. Thus $\alpha^2 \notin \mathbb{Q}$. Similarly, b is nonzero (otherwise $f(x)$ is reducible) so none of the roots are 0 and $\alpha \pm \beta \notin \mathbb{Q}$ either.

(b) (i) The resolvent cubic for $f(x)$ is $h(x) = x^3-2ax^2+(a^2-4bx) = x(x^2-2ax+a^2-4b)$. The solutions to the quadratic term are $(1/2)(2a \pm \sqrt{4a^2-4(a^2-4b)}) = (a \pm \sqrt{a^2-(a^2-4b)}) = a \pm 2\sqrt{b}$. Note $G \cong V$ if and only if $h(x)$ splits into linear factors, which is true if and only if $\sqrt{b} \in \mathbb{Q}$ so b is a square. Note also that if $G \cong V$ then every element of G has order 2 so we must have $\alpha\beta \in \mathbb{Q}$. Conversely, if $\alpha\beta \in \mathbb{Q}$ then $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leq 4$ so G must be isomorphic to V since given the factorization of $h(x)$ it cannot be isomorphic to C.

(ii) Note that the discriminant $D = 16a^4b-128a^2b^2+256b^3 = 16b(a^2-4b)^2$. Note that $G \cong C$ if and only if $f(x)$ is reducible over $\mathbb{Q}(\sqrt{D})$ since $h(x)$ has a linear factor. But given the value of D, this is true if and only if $b(a^2-4b)$ is a square. Additionally, we know that if $G \cong C$ then $\alpha\beta \notin \mathbb{Q}$ but since $[\mathbb{Q}(\alpha\beta):\mathbb{Q}] = 4$ we see that $\alpha\beta \in \mathbb{Q}(\alpha^2)$. The converse is true by the same degree considerations.

(iii) This follows from the other two parts since the only possibilities for G are V, C and D_8 since $h(x)$ factors. Thus, $G \cong D_8$ if and only if G is not V and G is not C if and only if b and $b(a^2-4b)$ are not squares if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$. □