MATH 3030, Abstract Algebra
Winter 2013
Toby Kenney
Homework Sheet 17
Model Solutions

Basic Questions

1. *(a) Is the regular 120-gon constructable?*

   $120 = 2^3 \times 3 \times 5$. 3 and 5 are Fermat primes, so the regular 120-gon is constructable.

   (b) Is the regular 28-gon constructable?

   $28 = 2^2 \times 7$. 7 is not a Fermat prime, so the regular 28-gon is not constructable.

   (c) Is the regular 100-gon constructable?

   $100 = 2^2 \times 5^2$, so the regular 100-gon is not constructable, since 100 is divisible by 5^2.

2. *Show that if m and n are distinct, and not divisible by p, then $\Phi_m(x)$ and $\Phi_n(x)$ have no common factor in $\mathbb{Z}_p[x]$.*

   Let α be a primitive mth root of unity in $\mathbb{Z}_p[x]$, and let β be a primitive nth root of unity. We have that $\Phi_m(x) = \mathrm{Irr}(\alpha, \mathbb{Z}_p)$ and $\Phi_n(x) = \mathrm{Irr}(\beta, \mathbb{Z}_p)$. Since these are irreducible in $\mathbb{Z}_p$, if they have a common factor, then they must be equal. However, $\Phi_m(x)$

3. *(a) Let K be the splitting field of the polynomial $f(x) = x^3 + x^2 + 2$ over $\mathbb{Z}_3$. Is K a radical extension of $\mathbb{Z}_3$?*

   We know that f divides $x^{27} - x$, so all elements of f are in GF(27), so K must be GF(27). Therefore, $[K : \mathbb{Z}_3] = 3$. Therefore, to be a radical extension of $\mathbb{Z}_3$, K must be obtained by adjoining a cube root to $\mathbb{Z}_3$. However, all cube roots of elements in $\mathbb{Z}_3$ are in $\mathbb{Z}_3$, since every element of $\mathbb{Z}_3$ is a zero of $x^3 - x$. Therefore, there are no radical extensions of degree 3 over $\mathbb{Z}_3$, so K is not a radical extension of $\mathbb{Z}_3$.

   Alternatively: let α be a zero of f in K. Now by long division, we have $f(x) = (x-\alpha)(x^2 + (\alpha+1)x + \alpha^2 + \alpha)$. The other zeros of f are therefore $\alpha + 1 \pm \sqrt{\alpha + 1}$. We can find the square root of $\alpha + 1$ by solving

$$\begin{aligned}
(\alpha^2 + a\alpha + b)^2 &= \alpha + 1 \\
\alpha^4 + 2a\alpha^3 + (a^2 + 2b)\alpha^2 + 2ab\alpha + b^2 &= \alpha + 1 \\
(\alpha^2 + \alpha + 2) + 2a(2\alpha^2 + 1) + (a^2 + 2b)\alpha^2 + 2ab\alpha + b^2 &= \alpha + 1 \\
(1 + a + a^2 + 2b)\alpha^2 + (1 + 2ab)\alpha + 2 + 2a + b^2 &= \alpha + 1
\end{aligned}$$

The solution to these is $a = 1, b = 0$, so we have the square root of $\alpha + 1$ is $\alpha^2 + \alpha$, and the other zeros of f are $2\alpha^2 + 1$ and $\alpha^2 + \alpha + 1$, which are all in $\mathbb{Z}_3(\alpha)$. As above, we know that GF(27) is not a radical extension of $\mathbb{Z}_3$.

(b) is $f(x)$ solvable by radicals over $\mathbb{Z}_3$?

Yes, $f(x)$ is solvable by radicals over $\mathbb{Z}_3$. Even though K is not a radical extension, it is contained in GF(3^6), which is a radical extension — it is the 7th cyclotomic extension $\mathbb{Z}_3$.

4. *Find $\Phi_{12}(x)$ over $\mathbb{Q}$.*

We know that there are $\phi(12) = 4$ primitive 12th roots of unity. If we let ω be one such root, the others are ω^5, ω^7 and ω^{11}. We know that $x^{12} - 1 = (x^6 - 1)(x^6 + 1)$, so we know that $\Phi_{12}(x)$ is a factor of $(x^6 + 1)$. Furthermore, we know that i and $-i$ are non-primitive roots of unity, so we can remove a factor of $x^2 + 1$, to get $x^4 - x^2 + 1$. This is of degree 4, so must be the required polynomial.

Alternatively, we can directly compute the coefficients of $(x - \omega)(x - \omega^5)(x - \omega^7)(x - \omega^{11})$:

$$\begin{aligned}
\omega + \omega^5 + \omega^7 + \omega^{11} &= 0 \\
\omega^6 + \omega^8 + \omega^{12} + \omega^{12} + \omega^{16} + \omega^{18} &= 2 + \omega^4 + 2\omega^6 + \omega^8 \\
&= \omega^4 + \omega^8 \\
&= -1 \\
\omega^{13} + \omega^{17} + \omega^{19} + \omega^{23} &= 0 \\
\omega^{24} &= 1
\end{aligned}$$

to get $\Phi_{12}(x) = x^4 - x^2 + 1$

Theoretical Questions

5. *Show that for a field F of characteristic not dividing n, we have $x^n - 1 = \Pi_{d|n}\Phi_d(x)$. [The product is over all divisors of n.]*

Let ω be a primitive nth root of unity in $\overline{F}$. We know that $(x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}) = x^n - 1$. However, every ω^m is a primitive $\frac{n}{\gcd(m,n)}$th root of unity. So the product $\Pi_{d|n}\Phi_d(x)$ is equal to $\Pi(x - \omega^m)$, where the m ranges over all numbers such that $\frac{n}{\gcd(m,n)}$ divides n. Furthermore, $(x - \omega^m)$ cannot be a divisor of more than one $\Phi_d(x)$, since that would mean that ω^m would be a primitive d_1th root and a primitive d_2th root of unity, which isn't possible. However, all numbers m satisfy $\frac{n}{\gcd(m,n)}$ divides n, so this product is over all numbers 1 to n, so it is $x^n - 1$.

6. *Show that* $f(x) = x^5 - 9x + 6$ *is not solvable by radicals over* $\mathbb{Q}$.

We need to show that the Galois group is not solvable. Firstly, we note that f is irreducible by Eisenstein's criterion with $p = 3$. Therefore, the zeros of f are all conjugate, so the Galois group acts transitively on them. Next we observe that $f(x)$ has 3 real roots and two complex roots. We can see that $f(-\infty) = -\infty$, $f(0) = 6$, $f(1) = -2$, and $f(\infty) = \infty$, so by the intermediate value theorem, we see there are at least 3 real zeros. On the other hand, the roots can't all be real, since the sum of their squares is 0.

Alternatively, we use some basic calculus to see that $f'(x) = 4x^4 - 9$, so the only turning points for f are zeros of $x^4 - \frac{9}{4}$, which has only 2 real solutions.

Therefore, f has exactly 3 real solutions and two complex ones. Therefore its Galois group is a transitive subgroup of S_5, which contains a transposition, so it must be the whole of S_5, which is not solvable, so f is not solvable by radicals over $\mathbb{Q}$.

7. *Let* K *be a normal extension of* $\mathbb{Q}$ *with* $[K : \mathbb{Q}] = 26$. *Show that* K *is an extension of* $\mathbb{Q}$ *by radicals.* [You may assume that any group of order 26 contains an element of order 13.]

Claim. *Any group of order 26 contains an element of order 13.*

Proof. Let G be a group of order 26. It must have all elements of order 1, 2, 13 or 26. If all elements are of order 2, then consider two non-identity elements a and b. We can see that $\{e, a, b, ab\}$ is a subgroup, since ab is of order 2, so $abab = e$, so $aba = b$ and $ab = ba$. This is impossible, since 4 does not divide 26. Therefore, G must have an element of order 13. □

The Galois group of K over $\mathbb{Q}$ has order 26, so has an element of order 13. The cyclic subgroup generated by this element has index 2, so is normal, and the quotient group has order 2, so must be $\mathbb{Z}_2$. Therefore, we have shown that the Galois group is solvable.

8. *Let* f *be an irreducible cubic polynomial in* $\mathbb{Q}$ *with only one real root. Show that the Galois group of* f *is* S_3.

Since f is irreducible, its zeros are all conjugate, so the Galois group acts transitively on the zeros. Furthermore, since F has one real root, conjugation must fix that root and transpose the complex roots. Therefore, the Galois group is a transitive subgroup of S_3 containing a transposition. The only such subgroup is S_3 itself.