

MA30037 Galois Theory 2004, Sheet 7

Solutions

Geoff Smith, <http://www.bath.ac.uk/~masgcs>

1. Recall that a polynomial $f \in \mathbb{Z}[X]$ is *cyclotomic* if it is a factor (in $\mathbb{Z}[X]$) of $X^n - 1$.

(a) Find the factorizations into irreducible cyclotomic polynomials of $X^n - 1$ for $n \leq 14$.

Solution

- i. $n = 1$; $X - 1$
- ii. $n = 2$; $[X - 1][X + 1]$
- iii. $n = 3$; $[X - 1][X^2 + X + 1]$
- iv. $n = 4$; $[X - 1][X + 1][X^2 + 1]$
- v. $n = 5$; $[X - 1][X^4 + X^3 + X^2 + X + 1]$
- vi. $n = 6$; $[X - 1][X + 1][X^2 + X + 1][X^2 - X + 1]$
- vii. $n = 7$; $[X - 1][X^6 + X^5 + X^4 + X^3 + X^2 + X + 1]$
- viii. $n = 8$; $[X - 1][X + 1][X^2 + 1][X^4 + 1]$
- ix. $n = 9$; $[X - 1][X^2 + X + 1][X^6 + X^3 + 1]$
- x. $n = 10$; $[X - 1][X + 1][X^4 + X^3 + X^2 + X + 1][X^4 - X^3 + X^2 - X + 1]$
- xi. $n = 11$; $[X - 1][X^{10} + X^9 + \cdots + X + 1]$
- xii. $n = 12$; $[X - 1][X + 1][X^2 + 1][X^2 + X + 1][X^2 - X + 1][X^4 - X^2 + 1]$
- xiii. $n = 13$; $[X - 1][X^{12} + X^{11} + \cdots + X + 1]$
- xiv. $n = 14$; $[X - 1][X + 1][X^6 + X^5 + \cdots + X + 1][X^6 - X^5 + \cdots - X + 1]$

(b) Find the smallest n such that $X^n - 1$ has an irreducible cyclotomic factor which has a coefficient which is neither, 1, -1 nor 0. *You*

should only attempt this question if you have access to a suitable computer algebra system.

Solution $105(= 3 \times 5 \times 7)$.

2. Let P_1, P_2, \dots, P_n ($n \geq 2$) be the vertices of a regular n -gon inscribed in a circle of unit radius. Show that the product of all the distances $|P_i P_j|$ is $\sqrt{n^n}$, *Hint: reassure yourself by looking at small values of n , and then consider the polynomial $(X + 1)^n - 1$ and its roots in \mathbb{C} .*

Solution The modulus of the product of the complex roots of $X^{n-1} + nX^{n-2} + \dots + n$ is n . This is also the product of all lengths of sides and diagonals of the regular n -gon with one end specified. Multiplying over all possible end vertices we get n^n , but every side and diagonal has been counted twice in this product so the correct answer is $\sqrt{n^n}$,

3. Which of the following polynomials are irreducible in $\mathbb{Q}[X]$?

(a) $X^{42} + 169X - 91$.

Solution Irreducible by EC, using $p = 13$.

(b) $X^4 + 4X^3 + 9X^2 + 16X + 16$.

Solution Replace X by $X - 1$ and get $X^4 + 3X^2 + 6X + 6$ which is irreducible by EC using $p = 2$.

(c) $X^4 + 4$.

Solution $X^4 + 4 = [X^4 + 4X^2 + 4] - 4X^2 = [X^2 + 2]^2 - [2X]^2 = [X^2 - 2X + 2][X^2 + 2X + 2]$

(d) $X^4 + 4X^3 + 6X^2 + 4X + 5$.

Solution $(X+1)^4+4$ is not irreducible because X^4+4 is reducible.

4. Suppose that n is a natural number. Show that there is a field K such that $\mathbb{Q} \leq K$ and $|K : \mathbb{Q}| = n$. Provided that you believe Gauss's *Fundamental Theorem of Algebra*, show that one may choose K to be a subfield of \mathbb{C} .

Solution $X^n - 2$ is irreducible by EC. Let α be a complex n -th root of 2 then $|\mathbb{Q}(\alpha) : \mathbb{Q}| = n$.

5. Show that there are infinitely many pairwise non-isomorphic fields $K \leq \mathbb{C}$ such that $|K : \mathbb{Q}| = 2$.

Solution Consider the fields $\mathbb{Q}(\sqrt{p})$ where p is prime. These are extensions of the rationals of degree 2, Now $X^2 - q$ is reducible in

$\mathbb{Q}(\sqrt{p})[X]$ but (we claim) irreducible in $\mathbb{Q}(\sqrt{q})[X]$ when $q \neq p$. This is because $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})[X]$, for if $\sqrt{p} = a + b\sqrt{q}$ with rational a and b , then $(\sqrt{p} - b\sqrt{q})^2$ would be rational so $2b\sqrt{pq}$ would be rational so $\sqrt{pq} \in \mathbb{Q}$ which is not true (why?).

6. Suppose that $f \in \mathbb{Q}[X]$ is irreducible, and that $\alpha, \beta \in \mathbb{C}$ are roots of f .

(a) Prove that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are isomorphic fields.

Solution They are both isomorphic to $\mathbb{Q}[X]/(f)$.

(b) Show that it need not be the case that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Solution Let $f = X^3 - 2$. Let $\omega = e^{\frac{2\pi i}{3}}$. Let $\alpha = \sqrt[3]{2}$ and $\beta = \omega\sqrt[3]{2}$. Now $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ but $\omega \notin \mathbb{R}$ so $\mathbb{Q}(\beta) \not\subseteq \mathbb{R}$. Therefore $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$.