MA-414 (Galois Theory)
Tutorial-8

March 11, 2023

1. Let m and n be coprime integers. Show that $\mathbb{Q}[\zeta_n, \zeta_m] = \mathbb{Q}[\zeta_{mn}]$.

2. Let $m, n > 1$ be integers and let l be their lcm. Show that $\mathbb{Q}[\zeta_n, \zeta_m] = \mathbb{Q}[\zeta_l]$.

3. Let $\Phi_n(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta_n^i)$ denote the nth cyclotomic polynomial. Show that
$$X^n - 1 = \prod_{d|n} \Phi_d(X)\,.$$

4. Let p be prime. Show that $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.

5. Let $n = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l}$. Let $m = p_1 p_2 \dots p_l$. Show that
$$\Phi_n(X) = \Phi_m(X^{n/m})\,.$$

6. If $n > 1$ is odd then $\Phi_{2n}(X) = \Phi_n(-X)$.

7. If p is a prime not dividing n then $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$. If p divides n then $\Phi_{pn}(X) = \Phi_n(X^p)$.

8. Define the Möbius μ-function by
$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ has a square factor,} \\ (-1)^r & \text{if } n \text{ has } r \text{ distinct prime factors.} \end{cases}$$
Let $\mathbb{N}$ be the set of all positive integers. Let $f : \mathbb{N} \to \mathbb{N}$ be a function, and define
$$F(n) := \sum_{d|n} f(d), \quad \forall\, n \in \mathbb{N}\,.$$
The *Möbius inversion formula* states that one can recover the function $f(n)$ from $F(n)$ by
$$f(n) = \sum_{d|n} \mu(d) F(n/d), \quad \forall\, n \in \mathbb{N}\,.$$
Use the Möbius inversion formula to show that
$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}\,.$$

9. Let p be a primes and let $n > 1$ be an integer such that $p \nmid n$. For $a \in \mathbb{Z}$, we get an integer $\Phi_n(a) \in \mathbb{Z}$, since $\Phi_n(X) \in \mathbb{Z}[X]$. Show that $p|\Phi_n(a)$ iff the order of a in $(\mathbb{Z}/p\mathbb{Z})^\times$ is equal to n.

10. Let $f(X) \in \mathbb{Z}[X]$ be a polynomial whose constant coefficient is 1. Let S_N be the set of those primes which divides any member of the set $\{f(n) \,|\, n \geq N\}$. Show that $\#S_N$ is infinite.

11. Let $f(X) \in \mathbb{Z}[X]$. Let S_N be the set of those primes which divides any member of the set $\{f(n) \,|\, n \geq N\}$. Show that $\#S_N$ is infinite.

12. Let $f(X) = \Phi_n(X)$ and apply the previous exercise. Show that there are infinitely many primes p such that $n|(p-1)$. This is a special case of Dirichlet's Theorem.

13. Use the previous exercise to give a complete proof of the fact that every finite abelian group occurs as the Galois group of an extension of $\mathbb{Q}$.

14. Let $a \in \mathbb{Z}$. Show that if p is an odd prime dividing $\Phi_n(a)$, then either $p \mid n$ or $n \mid (p-1)$.

15. Let $p > 2$ be a prime number and $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$, where $i = \sqrt{-1}$. Let L be a subfield of $\mathbb{Q}(\zeta_p)$ such that $[L : \mathbb{Q}] = \frac{1}{2}(p-1)$. Show that $L = \mathbb{Q}(\zeta_p + \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$.

16. Show that $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$. Prove the following.

    (a) If $p \equiv 1 \mod 4$, show that $\sqrt{p} \in \mathbb{Q}(\zeta_p)$. (HINT: Use $\zeta_p^i = \zeta_p^{p-(p-i)}$)

    (b) If $p \equiv 3 \mod 4$, show that $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$.

    (c) Show that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

17. Use the above two exercises to show that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

18. Let $p, q > 0$ be two distinct prime numbers. Show that $\mathbb{Q}(\zeta_p^m) \cap \mathbb{Q}(\zeta_q^n) = \mathbb{Q}$, for any two positive integers n, m.

19. Let $n = p_1^{r_1} \cdots p_m^{r_m}$ be the unique decomposition of a positive integer $n \geq 2$ into product of distinct prime powers. Show that

    (a) $\mathbb{Q}(\zeta_n) = \prod_{j=1}^{m} \mathbb{Q}(\zeta_{p_j{}^{r_j}})$, and

    (b) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_{j=1}^{m} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_j{}^{r_j}})/\mathbb{Q})$.

20. For an integer $n > 0$, let ζ_n be the primitive n-th root of unity. Let $r > 0$ be an integer with $\gcd(r, n) = 1$. Let $\sigma_r \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ be such that $\sigma_r(\zeta_n) = \zeta_n^r$. Show that, $\sigma_r(\zeta) = \zeta^r$, where ζ is a n-th root of unity.

21. Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not contained in any cyclotomic extension of $\mathbb{Q}$.

22. Prove that the set of all primitive n-th roots of unity form a basis over $\mathbb{Q}$ of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n-th roots of unity if and only if n is *square free* (that is, n is not divisible by square of any prime number).

23. Let $n \geq 1$ be an integer, and let $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the *Frobenius automorphism* define by $\sigma_p(a) = a^p$, for all $a \in \mathbb{F}_{p^n}$. Consider $\mathbb{F}_{p^n}$ as a $\mathbb{F}_p$-vector space and σ_p a $\mathbb{F}_p$-linear transformation.

    (a) Find the characteristic polynomial of σ_p.

    (b) Show that the $\mathbb{F}_p$-linear map σ_p is diagonalizable over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ if and only if $\gcd(n, p) = 1$.