Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 649 - Abstract Algebra
Instructor: Professor Sasha Polishchuk

Homework - Week 5
ID: 952091294
Term: Spring 2025
Due Date: 7^{th} May 2025

Problem 13.3.5
The 5th cyclotomic field $\mathbb{Q}(\zeta_5)$ contains $\sqrt{5}$.

Solution: Let ζ_5 be a 5th primitive root of $x^5 - 1$. The cyclotomic field $\mathbb{Q}(\zeta_5)$ contains all 5 roots: $1, \zeta^5, \zeta_5^2, \zeta_5^3, \zeta_5^4$. Write $\zeta_5 + \zeta_5^4 = e^{2\pi i/5} + e^{8\pi i/5} \in \mathbb{Q}(\zeta_5)$. On the other hand, we can calculate that

$$\zeta_5 + \zeta_5^4 = e^{2\pi i/5} + e^{-2\pi i/5} = 2\cos(\frac{2\pi}{5}).$$

By calculation, we know that

$$\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}.$$

This implies

$$\sqrt{5} = 2(\zeta_5 + \zeta_5^4) + 1 \in \mathbb{Q}(\zeta_5).$$

Problem 13.3.7
If p is a prime then

$$\Phi_{p^n}(x) = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}}.$$

Solution: We know by definition of the cyclotomic polynomial that

$$x^{p^n} - 1 = \prod_{d \mid p^n} \Phi_d(x),$$
$$x^{p^{n-1}} - 1 = \prod_{d \mid p^{n-1}} \Phi_d(x).$$

The only number that divides p^n but does not divide p^{n-1} is p^n. Thus, we can write

$$\Phi_{p^n}(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1}.$$

It is easy to check that

$$(1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}})(x^{p^{n-1}} - 1) = x^{p^n} - 1.$$

Since $\mathbb{Q}[x]$ is a UFD, we can conclude that

$$\Phi_{p^n}(x) = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}}.$$

Problem 13.3.9
$\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic extension of $\mathbb{Q}$.

Solution: The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2. Let $\mathbb{F}$ be the splitting field of x^3-2, then $\mathbb{F}$ is the smallest Galois extension containing a subextension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We have calculated in a previous exercise that the Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) \cong S_3$, which is not Abelian. But the Galois group of any cyclotomic extension is Abelian, and S_3 cannot be realized as a quotient group of an Abelian group. This implies that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic extension of $\mathbb{Q}$.

Problem 13.5.2
Let $\mathbb{K}/\mathbb{k}$ be a field extension. If $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ is algebraically independent over $\mathbb{k}$, and $\alpha \notin \mathbb{k}$ is the element of $k(\alpha_1, \ldots, \alpha_n)$, then α is transcendental over $\mathbb{k}$.

Solution: By Theorem 13.5.1, $\alpha \in \mathbb{k}(\alpha_1, \ldots, \alpha_n) \cong \mathbb{k}(x_1, \ldots, x_n)$. So α can be written as a ratio of two polynomials $p, q \in \mathbb{k}[x_1, \ldots, x_n]$ where $\deg p + \deg q \geq 1$. Suppose α is algebraic over $\mathbb{k}$, then there exists $f \in \mathbb{k}[x]$ such that $f(\alpha) = 0$. This implies that $f(\frac{p}{q}) = 0$. Note that $f(\frac{p}{q})$ is still in $\mathbb{k}(x_1, \ldots, x_n)$, so it can be written as

$$0 = f(\frac{p}{q}) = \frac{p'}{q'}$$

where $p', q' \in \mathbb{k}[x_1, \ldots, x_n]$. Now we know that $p' = 0$. This is the same as saying $p'(\alpha_1, \ldots, \alpha_n) = 0$. This shows that $\alpha_1, \ldots, \alpha_n$ are algebraically dependent over $\mathbb{k}$. A contradiction. Thus, α is transcendental over $\mathbb{k}$.

Problem 13.5.4
If β is algebraic over $\mathbb{k}(\alpha)$ and β is transcendental over $\mathbb{k}$ then α is algebraic over $\mathbb{k}(\beta)$.

Solution: Suppose α is transcendental over $\mathbb{k}(\beta)$. Since $\mathbb{k}(\beta)/\mathbb{k}$ is a transcendental field extension, by the Main Criterion, we know that the set $\{\alpha, \beta\}$ is algebraically independent. Use the Main Criterion again, and we have shown that β is transcendental over $\mathbb{k}(\alpha)$. This is a contradiction.

Problem 13.5.19
Let $\mathbb{k} \subsetneq \mathbb{F} \subseteq \mathbb{k}(x)$ be field extensions, with x transcendental over $\mathbb{k}$. Then $\mathbb{k}(x)/\mathbb{F}$ is finite.

Solution: Suppose $\mathbb{F}/\mathbb{k}$ is algebraic. Choose an element $\alpha \in \mathbb{F} \subseteq \mathbb{k}(x)$ but $\alpha \notin \mathbb{k}$, then $\alpha = \frac{p(x)}{q(x)}$ where $p(x), q(x) \in \mathbb{k}[x]$. α being algebraic over $\mathbb{k}$ implies that there exists a polynomial $F(x) \in \mathbb{k}[x]$ such that $F(\alpha) = 0$. This can be written as $F(\frac{p(x)}{q(x)}) = 0$. Note that $F(\frac{p(x)}{q(x)})$ is still in $\mathbb{k}(x)$, so it can be written as

$$0 = F(\frac{p(x)}{q(x)}) = \frac{p'(x)}{q'(x)}$$

where $p'(x), q'(x) \in \mathbb{k}[x]$. This implies that $p'(x) = 0$ for some polynomial p' and x is algebraic over $\mathbb{k}$. A contradiction. So $\mathbb{F}/\mathbb{k}$ is a transcendental field extension. By the Tower Law for transcendental degree, $\Bbbk(x)/\mathbb{F}$ is algebraic. x being algebraic over $\mathbb{F}$ implies there exists $g(y) \in \mathbb{F}[y]$ such that $g(x) = 0$. This tells us that $[\Bbbk(x) : \mathbb{F}] \leq \deg g < \infty$ is finite. So $\Bbbk(x)/\mathbb{F}$ is a finite field extension.

Problem 13.6.5 (Newton's identities)
Let $x_1, \ldots, x_n$ be variables, and define power sum symmetric functions

$$p_k = p_k(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k \quad (k \in \mathbb{Z}_{>0}).$$

Prove the *Newton identities*:

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i$$

where e_k are the elementary symmetric functions interpreted 1 if $k = 0$ and as 0 if $k > n$. Deduce that every elementary symmetric function e_k can be written down as a polynomial in $p_1, \ldots, p_k$ with rational coefficients. Deduce that every symmetric polynomial can be written down as a polynomial in the power sum symmetric functions.

Solution: Let $x_1, \ldots, x_n$ be variables, define the following polynomial

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n).$$

Remove the parentheses, and we can rewrite $f(x)$ as

$$f(x) = x^n - e_1 x^{n-1} + \cdots + (-1)^{n-1} e_{n-1} x + (-1)^n e_n.$$

We prove Newton's identities in different cases.

(a) Suppose $k = n$.
We know that for $1 \leq i \leq n$, x_i is the root of f, so it satisfies the following equation.

$$x_i^n - e_1 x_i^{n-1} + \cdots + (-1)^{n-1} e_{n-1} x + (-1)^n e_n = 0. \tag{1}$$

Add all these equations from $i = 1$ to $i = n$, we obtain

$$p_n - e_1 p_{n-1} + \cdots + (-1)^{n-1} e_{n-1} p_1 + (-1)^n n e_n = 0.$$

This is the same as

$$\begin{aligned}(-1)^{n-1} n e_n &= \sum_{i=1}^{n} (-1)^{n-i} e_{n-i} p_i \\ n e_n &= \sum_{i=1}^{n} (-1)^{i-1} e_{n-i} p_i.\end{aligned}$$

(b) Suppose $k > n$.
Let $\alpha_1, \alpha_2, \ldots, \alpha_{k-n}$ be a variable. Consider the polynomial

$$g(x) = f(x)(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{k-n}).$$

In this case, the generic polynomial is e'_j and the power sum function is p'_j for $1 \leq j \leq k$. From the result in (a), we have an equation

$$ke'_k = \sum_{i=1}^{k}(-1)^{i-1}e'_{k-i}p'_i.$$

Let $\alpha_1 = \alpha_2 = \cdots = \alpha_{k-n} = 0$. Then we have

$$e'_j = e_j, \qquad \text{if } 1 \leq j \leq n, \tag{2}$$
$$e'_j = 0, \qquad \text{if } n+1 \leq j \leq k, \tag{3}$$
$$p'_j = p_j, \qquad \text{if } 1 \leq j \leq k. \tag{4}$$

Then the equation can be rewritten as

$$0 = ke_k = \sum_{i=1}^{k}(-1)^{i-1}e_{k-i}p_i.$$

(c) Suppose $k < n$.
Consider the formal derivative $f'(x)$ of $f(x)$, which can be written in two forms:

$$f'(x) = \sum_{j=1}^{n}\frac{f(x)}{x-x_j},$$
$$f'(x) = nx^{n-1} - (n-1)e_1x^{n-2} + \cdots + (-1)^{n-1}e_{n-1}.$$

For $0 \leq l \leq n-1$, the coefficient in front of x^{n-1-l} is $(-1)^l(n-l)e_l$. For $1 \leq j \leq n$, $\frac{f(x)}{x-x_j}$ can be written as

$$\frac{f(x)}{x-x_j} = (x-x_1)\cdots(x-x_{j-1})(x-x_{j+1})\cdots(x-x_n).$$

Remove the parentheses, and we obtain

$$\begin{aligned}\frac{f(x)}{x-x_j} =& x^{n-1} + (-e_1+x_j)x^{n-2} + (e_2 - e_1x_j + x_j^2)x^{n-3} \\ & + \cdots + ((-1)^le_l + \sum_{m=1}^{l}(-1)^{l+m}e_{l-m}x_j^m)x^{n-l-1} + \cdots \\ & + (-1)^{n-1}e_{n-1} + \sum_{m=1}^{n-1}(-1)^{m+n-1}e_{n-m-1}x_j^m.\end{aligned}$$

Add $j=1$ to $j=n$ together, and we have

$$f'(x) = nx^{n-1} + \sum_{l=1}^{n-1}[(-1)^lne_l + (\sum_{m=1}^{l}(-1)^{l+m}e_{l-m}p_m)]x^{n-l-1}$$

Comparing coefficients, and we have, for $1 \leq l \leq n-1$,

$$(-1)^l (n-l) e_l = (-1)^l n e_l + \sum_{m=1}^{l} (-1)^{l+m} e_{l-m} p_m.$$

This is equivalent to

$$l e_l = \sum_{m=1}^{l} (-1)^{m-1} e_{l-m} p_m$$

for all $1 \leq l \leq n-1$.

We have proved Newton's identities for $k > 0$. We have

$$\begin{aligned} e_1 &= p_1, \\ 2e_2 &= e_1 p_1 - p_2, \\ 3e_3 &= e_2 p_1 - e_1 p_2 + p_3, \\ &\cdots \end{aligned}$$

for all $k > 0$. From this, we can inductively write e_k as a polynomial of $p_1, \ldots, p_k$ with rational coefficients. By Theorem 13.6.1, since every symmetric polynomial can be written down as a polynomial in symmetric functions, then it can also be written as a polynomial in power sum functions.