Assignment-IIB

Galois Theory

Trishan Mondal

§ Problem 1

Determine the Galois groups of the following polynomials:

1. $x^3 - x^2 - 4$
2. $x^3 + x^2 - 2x - 1$

(1) We can factorize the polynomial $f(x) = x^3 - x^2 - 4$ as following,

$$f(x) = (x-2)(x^2 + x + 2)$$

The quadratic factor is irreducible over $\mathbb{Q}$ so the Galois group of f is, $\text{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

(2) The polynomial $f(x) = x^3 + x^2 - 2x - 1$ don't have any factor over $\mathbb{Q}$ as by rational root test it don't have any root over $\mathbb{Q}$. The reduced polynomial will be,

$$\begin{aligned}\tilde{f}(x) &= f\left(x - \frac{1}{3}\right) \\ &= x^3 - \frac{7x}{3} - \frac{11}{27}\end{aligned}$$

$\tilde{f}$ is also irreducible (as f is) and discriminant is

$$D(f) = -4.\left(-\frac{7}{3}\right)^3 - 27.\left(-\frac{11}{27}\right)^2 = \frac{417}{9}$$

This is not a square in $\mathbb{Q}$. So $\text{Gal}(f) = S_3$.

§ Problem 2

Find the Galois groups of the following quartics:

1. $x^4 + 3x^3 - 3x - 2$
2. $x^4 + 2x^2 + x + 3$
3. $x^4 + 4x - 1$

(1). Done is **Assignment II(A)**.

(2). Let, $f(x) = x^4 + 2x^2 + x + 3$. Check this polynomial mod 2. $\bar{f} = x^4 + x + 1$. This polynomial is irreducible. $\bar{f}$ don't have any linear factor over $\mathbb{Z}/2\mathbb{Z}$. If it had quadratic factor $(x^2 + a_1 x + b_1)(x^2 + a_2 x + b_2) = \bar{f}$ then, $b_1 b_2 = 1$ i.e. $b_1 = b_2 = 1$. From the coefficient of x^3, x^1 we get, $a_1 + a_2 = 0$ and $a_1 b_2 + b_1 a_2 = 1$.

But this is not possible (by putting $b_1 = b_2 = 0$). Thus $f(x)$ is irreducible. The resolvent cubic of this polynomial is,

$$h(x) = x^3 - 4x^2 - 8x + 1$$

it is irreducible by rational root test, discriminant of the polynomial is 3877, it's not a square in $\mathbb{Q}$. So the Galois group $\mathrm{Gal}(f) \simeq S_4$.

(3). Let, $f(x) = x^4 + 4x - 1$. By rational root test this polynomial don't have any root over $\mathbb{Q}$ thus, f don't have any linear factor over $\mathbb{Q}$. Let's check mod 3, $\bar{f} = x^4 + x - 1$. It doesn't have linear factor mod 3, if it had two quadratic factors then $(x^2 + a_1x + b_1)(x^2 + a_2x + b_2) = \bar{f}$, then $b_2b_1 = -1$ i.e (WLOG) $b_1 = 1, b_2 = -1$. $a_2b_1 + b_2a_1 = 1$ and $a_1 + a_2 = 0$ mod 3, which means we have $a_2 = 2$ and $a_1 = 1$. From the coefficient of x^2 we can say

$$a_1a_2 + b_1 + b_2 = 0$$

but it's not the case for the values we got for a_i, b_i. So f is irreducible (as $\bar{f}$ is). Now the resolvent polynomial is,

$$h(x) = x^3 + 4x + 16 = (x + 2)(x^2 - 2x + 8)$$

discriminant of the quadratic factor is $\sqrt{7}i$. It is not hard to see $f(x)$ is irreducible over $\mathbb{Q}(\sqrt{7}i)$, so $\mathrm{Gal}(f) \simeq D_8$.x

§ Problem 3

1. Let $\alpha, -\alpha, \beta, -\beta$ 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 $\alpha^2, \alpha + \beta$ and $\alpha - \beta$ are not elements of $\mathbb{Q}$.
2. Suppose $f(x)$ is irreducible and let G be the Galois group of $f(x)$. Prove that
   (a) $G \cong V_4$, if and only if b is a square in $\mathbb{Q}$ if and only if $\alpha\beta$ is rational.
   (b) $G \cong \mathbb{Z}_4$, if and only if $b(a^2 - 4b)$ is a square in $\mathbb{Q}$ if and only if $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.
   (c) $G \cong D_8$, if and only if b and $b(a^2 - 4b)$ are not squares in $\mathbb{Q}$ if and only if $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

(1). If the polynomial $f = x^4 + ax^2 + b$ is irreducible over $\mathbb{Q}$, then it can't have any linear factor so none of $\alpha, \beta \in \mathbb{Q}$. It also can't have any quadratic factor over $\mathbb{Q}$. Only possible quadratic factorization of f are $(x^2 - \alpha^2)(x^2 - \beta^2), (x^2 \pm (\alpha + \beta)x + \alpha\beta)(x^2 \pm (\alpha - \beta)x - \alpha\beta)$. Irreducibility of f implies $\alpha^2 \notin \mathbb{Q}$.

Conversely, if $\alpha^2 \in \mathbb{Q}$ then $f(x) = \left(x^2 - \alpha^2\right)\left(x^2 - \beta^2\right)$, and if $\alpha \pm \beta \in \mathbb{Q}$ then $\alpha^2 + \beta^2 \pm \alpha\beta \in \mathbb{Q}$, but since $\alpha^2 + \beta^2 = -a \in \mathbb{Q}$ this implies $\alpha\beta \in \mathbb{Q}$ and so $f(x) = \left(x^2 + (\alpha - \beta) - \alpha\beta\right)\left(x^2 + (-\alpha + \beta) - \alpha\beta\right)$ or $f(x) = \left(x^2 - (\alpha + \beta) + \alpha\beta\right)\left(x^2 + (\alpha + \beta) + \alpha\beta\right)$ is a factorization in $\mathbb{Q}[x]$.

(2). The resolvent cubic of $f(x)$ is $r(x) = (x - a)\left(x^2 - 4b\right)$ and it is reducible by the algorithm of the Galois group of a quartic the Galois group G of $f(x)$ is either $V = \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4$ or D_8.

(a) Note that r splits completely over $\mathbb{Q}$ if and only if $\sqrt{b} \in \mathbb{Q}$, if and only if $\alpha\beta \in \mathbb{Q}$ (since $b = \alpha^2\beta^2$). Therefore $G \cong V_4$ if and only if b is a square in $\mathbb{Q}$ if and only if $\alpha\beta \in \mathbb{Q}$.

(b) Suppose r has a unique root in $\mathbb{Q}$, which in particular we know is a, also note that the splitting field of $r(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{b})$. Then consider the polynomial $h(x) = x^2\left(x^2 - ax + b\right)$. If h splits over $\mathbb{Q}(\sqrt{b})$, then we would have $\sqrt{a^2 - 4b} \in \mathbb{Q}(\sqrt{b})$. Now

$$\sqrt{a^2 - 4b} = x + y\sqrt{b} \Rightarrow \left(a^2 - 4b\right) + y^2b - 2y\sqrt{b\left(a^2 - 4b\right)} = x^2 \Rightarrow \sqrt{b\left(a^2 - 4b\right)} = \frac{a^2 - 4b + y^2b - x^2}{2y} \in \mathbb{Q}.$$

Conversely if $\sqrt{b\left(a^2-4b\right)} \in \mathbb{Q}$ then we get $\sqrt{b\left(a^2-4b\right)} = x \in \mathbb{Q} \Rightarrow \sqrt{a^2-4b} \in \mathbb{Q}(\sqrt{b})$, and hence h will split completely over $\mathbb{Q}(\sqrt{b})$. Therefore $G \cong \mathbb{Z}/4\mathbb{Z}$ if and only $\sqrt{b\left(a^2-4b\right)} \in \mathbb{Q}$, if and only if $\mathbb{Q}\left(\sqrt{a^2-4b}\right) = \mathbb{Q}(\sqrt{b})$.

Note that $a^2-4b = \left(\alpha^2+\beta^2\right)^2 - 4\alpha^2\beta^2 = \left(\alpha^2-\beta^2\right)^2$. Thus $\sqrt{a^2-4b} = \alpha^2-\beta^2$. While $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\alpha\beta)$. Then $\alpha^2-\beta^2 \in \mathbb{Q}(\alpha\beta)$ if and only if $\alpha^2 = \frac{1}{2}\left[\left(\alpha^2-\beta^2\right)+\left(\alpha^2+\beta^2\right)\right] \in \mathbb{Q}(\alpha\beta)$ (since $\alpha^2+\beta^2 \in \mathbb{Q}$)). But clearly $\alpha^2 \notin \mathbb{Q}$, since f is irreducible, thus we must have $\mathbb{Q}\left(\alpha^2\right) = \mathbb{Q}(\alpha\beta)$. Conversely if $\mathbb{Q}\left(\alpha^2\right) = \mathbb{Q}(\alpha\beta)$ then we get that $\alpha^2-\beta^2 \in \mathbb{Q}(\alpha\beta)$. Therefore from our previous observation we can say that $G \cong \mathbb{Z}/4\mathbb{Z}$ if and only if $\sqrt{b\left(a^2-4b\right)} \in \mathbb{Q}$ and $\sqrt{b} \notin \mathbb{Q}$, if and only if $\mathbb{Q}\left(\alpha^2\right) = \mathbb{Q}(\alpha\beta)$.

(c) It is evident from Case (b) that h does not split over $\mathbb{Q}(\sqrt{b})$ if and only if $\sqrt{b\left(a^2-4b\right)} \notin \mathbb{Q}$. Thus $G \cong D_4$ if and only if $\sqrt{b\left(a^2-4b\right)} \notin \mathbb{Q}$ and $\sqrt{b} \notin \mathbb{Q}$. And from our previous observation this can happen if and only if $\alpha\beta \notin \mathbb{Q}\left(\alpha^2\right)$.

§ Problem 4

Prove that the polynomial x^4+px+p over $\mathbb{Q}$ is irreducible for every prime p and for $p \neq 3, 5$, the Galois group is S_4. Prove that the Galois group for $p=3$ is D_8, and for $p=5$ it is D_8.

Solution. Done in **Assignment II(A)**.

§ Problem 5

Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Let s_i be the elementary symmetric function of degree i in the roots and define $s_i = 0$ for $i > n$. Let $p_i = \alpha_1^i + \cdots + \alpha_n^i, i \geq 0$, be the sum of the i^{th} powers of the roots of $f(x)$. Show that:

$$\begin{aligned}
&p_1 - s_1 = 0 \\
&p_2 - s_1p_1 + 2s_2 = 0 \\
&p_3 - s_1p_2 + s_2p_1 - 3s_3 = 0 \\
&\vdots \\
&p_i - s_1p_{i-1} + s_2p_{i-2} - \cdots + (-1)^{i-1}s_{i-1}p_1 + (-1)^i i s_i = 0
\end{aligned}$$

Solution. Let's denote $e_k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ as the elementary symmetric polynomial and $p_k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ as the power-sum symmetric polynomial, represented by:

$$\begin{aligned}
e_k(\alpha_1, \alpha_2, \cdots, \alpha_n) &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k} \\
p_k(\alpha_1, \alpha_2, \cdots, \alpha_n) &= \sum_{1 \leq i \leq n} \alpha_i^k
\end{aligned}$$

With these, the function $f(x)$ is defined as:

$$f(x) = \prod_{1 \leq i \leq n} (1 - \alpha_i x).$$

Vieta's formulas state that this expansion is given by:

$$f(x) = \sum_{k=0}^{n} (-1)^k e_k(\alpha_1, \cdots, \alpha_n) x^k.$$

Upon differentiation with respect to x and then multiplying by x, we obtain:

$$xf'(x) = \sum_{k=1}^{n}(-1)^k e_k k x^k$$

The above identity can also be written as:

$$x\frac{f'(x)}{f(x)} = -\left(\sum_{j=1}^{\infty} p_j x^j\right)$$

Expanding the polynomials on the right side gives:

$$-\left(\sum_{i=0}^{n}(-1)^i e_i x^i\right)\left(\sum_{j=1}^{\infty} p_j x^j\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k}(-1)^{i+1} e_i p_j\right) x^k$$

The summation extends from $0 \leq i \leq n$, with $e_i = 0$ for $i > n$ to avoid unnecessary summands. By equating the equations involving x's, we derive:

$$\sum_{k=1}^{n}(-1)^k e_k k x^k = \sum_{k=0}^{\infty}\left(\sum_{i+j=k}(-1)^{i+1} e_i p_j\right) x^k.$$

Equating the coefficients of x^r on both sides yields:

$$(-1)^r e_r r = \sum_{i+j=r}(-1)^{i+1} e_i p_j$$

Upon dividing both sides by $(-1)^r$, the equation becomes:

$$r e_r = \sum_{i+j=r}(-1)^{j+1} e_i p_j$$

§ Problem 6

1. Let $f(x)$ be a monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$. Show that the discriminant D of $f(x)$ is the square of the determinant of the Vandermonde matrix

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

which is $\prod_{i>j}(\alpha_i - \alpha_j)$.

2. Using the Vandermonde matrix above, multiplying on the left by its transpose and taking the determinant show that we obtain

$$D = \begin{vmatrix} p_0 & p_1 & p_2 & \cdots & p_{n-1} \\ p_1 & p_2 & p_3 & \cdots & p_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \cdots & p_{2n-2} \end{vmatrix}$$

where $p_i = \sum_{j=1}^{n} \alpha_j^i$ can be computed in terms of the coefficients of $f(x)$ using Newton's formulas above.

Solution. (1). We will prove this by induction on n. For the base case take $n = 1$, there is nothing to prove in that case. We are given transpose of the following matrix :

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n & \alpha_{n+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} & \alpha_{n+1}^{n-1} \\ \alpha_1^n & \alpha_2^n & \cdots & \alpha_n^n & \alpha_{n+1}^n \end{pmatrix}$$

By subtracting α_1 times the i-th row to the $i+1$-th row, we get

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 0 & \alpha_2 - \alpha_1 & \cdots & \alpha_n - \alpha_1 & \alpha_{n+1} - \alpha_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \alpha_2^n - \alpha_1\alpha_2^{n-1} & \cdots & \alpha_n^n - \alpha_1\alpha_n^{n-1} & \alpha_{n+1}^n - \alpha_1\alpha_{n+1}^{n-1} \end{pmatrix}$$

Expanding by the first column and factoring $\alpha_i - \alpha_1$ from the i-th column for $i = 2, \ldots, n+1$, you get the determinant is,

$$= \prod_{j=2}^{n+1}(\alpha_j - \alpha_1) \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_2 & \alpha_3 & \cdots & \alpha_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_{n+1}^{n-1} \end{pmatrix}$$

By applying inductive hypothesis we get:

$$= \prod_{j=2}^{n+1}(\alpha_j - \alpha_1) \prod_{2 \leqslant i < j \leqslant n+1} (\alpha_j - \alpha_i) = \prod_{1 \leqslant i < j \leqslant n+1} (\alpha_j - \alpha_i)$$

and the inductive step is complete. Thus the discriminant of the polynomial is square of the determinant of the Vandermonde matrix. ■

(2) Call the given matrix Vandermonde matrix A. Note that,

$$\begin{aligned}\left[A^T A\right]_{ij} &= \sum_{k=1}^{n} A_{ki}A_{kj} \\ &= \sum_{k=1}^{n} \alpha_k^{i-1}\alpha_k^{j-1} \\ &= \sum_{k=1}^{n} \alpha_k^{i+j-2}\end{aligned}$$

Thus determinant of the given matrix is $\det\left(A^T A\right) = \det(A)^2 = D$. ■

§ Problem 7

Prove that the discriminant of the cyclotomic polynomial $\Phi_p(x)$ of the p^{th} roots of unity for an odd prime p is $(-1)^{(p-1)/2}p^{p-2}$.

Solution. Note that, $D = (-1)^{(p-1)/2}\prod_{i\neq j}(\omega^i - \omega^j)$, where i, j varies over n (here D is discriminant) where ω is p^{th} root of unity. We know,

$$\Phi_p(X) = \prod_{i=1}^{p-1}\left(X - \omega^i\right)$$

and hence $\Phi_p'(X) = \sum_{i=1}^{p-1}\prod_{j\neq i}(X - \omega^j)$, $\Phi_p'(\omega^k) = \prod_{j\neq k}(\omega^k - \omega^j)$. Thus, $D = (-1)^{p-1/2}\prod_{i=1}^{p-1}\Phi_p'(\omega^i)$. Note that,

$$\begin{aligned}&(X-1)\Phi_p(X) = X^p - 1 \\ &\Rightarrow \Phi_p(X) + (X-1)\Phi_p'(X) = pX^{p-1} \\ &\Rightarrow (\omega^k - 1)\Phi_p'(\omega^k) = p\omega^{k(p-1)} \\ &\Rightarrow (-1)^{p-1/2}D = \prod_{k=1}^{p-1}\Phi_p'(\omega^k) = \prod_{k=1}^{p-1}\frac{p\omega^{k(p-1)}}{\omega^k - 1} \\ &= p^{p-1}(-1)^{p-1}\frac{\prod_{k=1}^{p-1}\omega^{-k}}{\Phi_p(1)} = p^{p-2}(-1)^{p-1} \\ &\Rightarrow D = (-1)^{p-1/2}p^{p-2}\end{aligned}$$

And hence we are done. ■

§ Problem 8

Prove that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p}) \subseteq \mathbb{Q}(\zeta_p)$ for p an odd prime.

Solution. We know square root of a discriminant lies in the splitting field. So by the previous problem we can say $\mathbb{Q}\left(\sqrt{(-1)^{p-1/2}p^{p-2}}\right) = \mathbb{Q}\left(\sqrt{(-1)^{p-1/2}p}\right)$ contained in splitting field of $\Phi_p(X)$, which is $\mathbb{Q}(\zeta_p)$. ■

§ Problem 9

Use the previous problem to prove that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Solution. We know any quadratic extension over field $\mathbb{Q}$ can be written as $\mathbb{Q}(\sqrt{d})$ for some square free integer $d \in \mathbb{Z}$. Let, $d = \pm p_1 \cdots p_r$ i.e.$\sqrt{d} = \sqrt{\pm 1}\sqrt{p_1} \cdots \sqrt{p_r}$, if all the primes are odd prime, then $\sqrt{d} \in \mathbb{Q}(\zeta_4, \zeta_{p_1}, \cdots, \zeta_{p_r})$. This follows from the previous result that $\sqrt{d}$ or $\sqrt{-d}$ is in the field, depending on the primes $p_1, \cdots, p_r$. Since ζ_4 is $\sqrt{-1}$ we can multiply it with the product so that we get $\sqrt{d}$. Since $4, p_1, \cdots, p_r$ are pairwise coprime we can say, $\mathbb{Q}(\zeta_4, \zeta_{p_1}, \cdots, \zeta_{p_r}) = \mathbb{Q}(\zeta_{4p_1 \cdots p_r})$.

If any of the prime is 2 (WLOG $p_1 = 2$), then we can see, $\sqrt{2}\sqrt{\pm p_2 \cdots p_r} \in \mathbb{Q}(\sqrt{2}, i, \zeta_{p_2}, \cdots, \zeta_{p_r})$. We know, $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ thus we have $\mathbb{Q}(\sqrt{2}, i, \zeta_{p_2}, \cdots, \zeta_{p_r}) = \mathbb{Q}(\zeta_{8p_1 \cdots p_r})$. So any quadratic extension is always contained in a cyclotomic extension. ■

§ Problem 10

Let $K = \mathbb{F}_p(t)$ be the field of rational functions, $f(x) = x^p - x - t \in K[x]$ and let E/K be the splitting field of $f(x)$. Prove that $\mathrm{Gal}(E/K) \cong \mathbb{Z}_p$ but that $f(x)$ is not solvable by radicals.

Solution. By a result in Assignment I(A). We can see $x^p - x - t$ is irreducible over $K = \mathbb{F}_p(t)$. If E is the splitting field of the polynomial then it contains a root α of f such that $f(\alpha) = 0$, it was also shown in Assignment I(A) that, $\alpha + 1, \cdots, \alpha + p - 1$ are also roots of f. Thus $E = K(\alpha)$ and $f' = -1$, thus the extension is separable and hence a Galois extension. So we have $|\mathrm{Gal}(f)| = p$ and $\sigma : E \to E$ the automorphism $\alpha \mapsto \alpha + 1$ is an element of $\mathrm{Gal}(f)$ with degree p. So, $\mathrm{Gal}(f)$ is cyclic group of order p i.e $\mathrm{Gal}(f) \simeq \mathbb{Z}_p$.

Let K be the splitting field of f over $F.K/F$ is Galois with degree p. If K lies in a radical extension L of F. Then we have

$$F = F_0 \subset F_1 \subset F_2 \ldots \subset F_r = L$$

where $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{n_i} \in F_{i-i}$. We may assume that $\alpha_i \notin F_{i-1}$ and n_i are all primes. Let K_i be $K(\alpha_1, \ldots \alpha_i)$, then $F_i \subset K_i$. By induction, we can prove that K_i/F_i is Galois with degree p as follows. First, K_0/F_0 is Galois with degree p. We assume K_{i-1}/F_{i-1} is Galois with degree $p.K_i = K_{i-1}(\alpha_i), F_i = F_{i-1}(\alpha_i)$. If $\alpha_i \in K_{i-1}$, then $F_i = F_{i-1}(\alpha_i) = K_i = K_{i-1}(\alpha_i) = K_{i-1}$ and $n_i = p$, since $[K_{i-1} : F_{i-1}] = p$. Because $\alpha_i \notin F_{i-1}, g = (t - \alpha_i)^p = t^p - \alpha_i^p$ is irreducible over F_{i-1}. Then the minimal polynomial of α_i over F_{i-1} is g. However, K_{i-1}/F_{i-1} is Galois, so α_i is separable, but $g = (t - \alpha_i)^p$, which shows that α_i is not separable.

This contradiction shows that $\alpha_i \notin K_{i-1}$. Note that $\alpha_i^{n_i} \in F_{i-1} \subset K_{i-1}$ and all n_i th roots of unity is in F. Then we have $g = t^{n_i} - \alpha_i^{n_i}$ is irreducible over K_{i-1} and $[K_i : K_{i-1}] = n_i$. Then we can conclude that K_i/F_i is Galois with degree p. By induction, K_i/F_i is Galois with degree p for all i. On the other hand, $K_r = F_r = L$, so K_r/F_r is of degree 1 , which leads to a contradiction.

§ Problem 11

Prove that the Galois group of $x^7 + 7x^4 + 14x + 3$ is A_7.

Solution. Let, $f(x) = x^7+7x^4+14x+3$. The discriminant of this polynomial is $D(f) = 4202539929$ which is square of 64827. So the Galois group of f will be contained in A_7. Check this polynomial mod 2, $\bar{f} = x^7+x^4+1$. This polynomial don't have any root over $\mathbb{Z}/2\mathbb{Z}$, if it was reducible mod 2 it must have a quadratic factor or a cubic factor, in the former case $\bar{f}$ must have a common factor with $x^4 - x$ but $\gcd(x^7 + x^4 + 1, x^4 + x) = 1$, in later case it must have a common factor with the polynomial $x^8 - x$. But

$$\begin{aligned}\gcd(x^7 + x^4 + 1, x^8 - x) &= \gcd(x^7 + x^4 + 1, x^8 + x) \\ &= \gcd(x^7 + x^4 + 1, x^7 + 1) = 1\end{aligned}$$

So f is irreducible over $\mathbb{Q}$. Note that f has the following factorization mod 5,

$$\bar{f} = (1 + x)(4 + x)(2 + x + 2x^2 + x^3 + x^5)$$

We claim that $x^5 + x^3 + 2x^2 + x + 2$ is irreducible over $\mathbb{F}_5$, it clearly does not have any linear factors. So its enough to show that $x^5 + x^3 + 2x^2 + x + 2$ does not have any quadratic factor over $\mathbb{F}_5[x]$. For the sake of contradiction suppose it has a quadratic factor over $\mathbb{F}_5$, then it would have a common factor with the polynomial $x^{25} - x = x\left(x^12 - 1\right)\left(x^{12} + 1\right)$. Thus it will have a common factor with either $x^{12} - 1$ or $x^{12} + 1$, but direct computation we get that

$$\gcd\left(x^{12} - 1, x^5 + x^3 + 2x^2 + x + 2\right) = \gcd\left(x^{12} + 1, x^5 + x^3 + 2x^2 + x + 2\right) = 1.$$

so our claim is proved. Since $5 \nmid D(f)$ by **Dedekind's** theorem we can say, $\mathrm{Gal}(f)$ contains a 5-cycle. From group theory we know the only transitive subgroup of A_7 containing a 5-cycle is A_7. So $\mathrm{Gal}(f) \simeq A_7$. ■

§ Problem 12

Prove that for each $n \in \mathbb{N}$ there exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ with Galois group S_n over $\mathbb{Q}$.

Solution. Let p_1 and p_2 be two different primes. Let f_1 be a n-degree irreducible polynomial of $\mathbb{Z}/p_1\mathbb{Z}[x]$, and f_2 be a $(n-1)$-degree polynomial in $\mathbb{Z}/p_2\mathbb{Z}[x]$ and f_4 is an irreducible quadratic, f_3 is $2\lfloor\frac{n-1}{2}\rfloor - 1$ degree irreducible polynomial over $\mathbb{Z}_{p_3}$. By CRT we know there is a polynomial f of degree n statisfying the following congruence relations :

$$\begin{aligned} f(x) &\equiv f_1 \pmod{p_1} \\ f(x) &\equiv x f_2 \pmod{p_2} \\ f(x) &\equiv x^{2\left\{\frac{n+1}{2}\right\}} f_4(x) f_3(x) \pmod{p_3} \end{aligned}$$

For the third case $\left\{\frac{n+1}{2}\right\}$ means the fractional part. Not that $2\left\{\frac{n+1}{2}\right\} + 2\lfloor\frac{n-1}{2}\rfloor + 1 = n$. We can see f is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$. By **Dedikind**'s theorem $\mathrm{Gal}(f)$ is a transitive subgroup of S_n containing a n-cycle and $(n-1)$-cycle and a transposition, i.e. $\mathrm{Gal}(f) \simeq S_n$. Since we have infinitely many choices of p_1, p_2, p_3 and corresponding choices of f_1, f_2, there are infinitely may polynomial f over $\mathbb{Z}$ having Galois group over $\mathbb{Q}$ as S_n. ■

Acknowledgement: While solving the Assignment I have discussed some problem with Soumya Dasgupta, Priyatosh Jana, Aaratrick Basu. Any other coincidence with my Solution is not my fault !!!