Assignment-1A

Galois Theory

Trishan Mondal
(Bmat 2144)

§ Problem 1

> **Problem.** Let K be an extension of F, and $\alpha \in K$ be algebraic over F. Show that the minimal polynomial of α over F is same as the minimal polynomial of the F-linear transformation $T_\alpha : K \to K$ defined by $T_\alpha(v) = \alpha v$ for all $v \in K$.

Proof. Let, $m_{F,\alpha}(x)$ be the minimal polynomial of α over F and $m_{T_\alpha}(x)$ be the minimal polynomial of the linear transformation T_α. Since, α is the eigenvalue of the linear transformation T_α we can say, $m_{T_\alpha}(\alpha) = 0$. Since, $m_{F,\alpha}$ is the monic, irreducible polynomial of minimal degree which has root α, $m_{F,\alpha}(x) \mid m_{T_\alpha}(x)$. For any $v \in K$ we can write,

$$m_{F,\alpha}(T_\alpha)(v) = m_{F,\alpha}(\alpha)(v) = 0$$

and hence, $m_{T_\alpha} | m_{F,\alpha}$. From here we can conclude that, $m_{T_\alpha}(x) = m_{F,\alpha}(x)$. ■

§ Problem 2

> **Problem.** Determine whether or not you can construct the following n-gons using straightedge and compass:
> (i) 5 -gon
> (ii) 9 -gon.

Solution. (i) **Regular 5-gon is constractible**. It is equivalent to show that, $\cos \frac{2\pi}{5}$ is constractible. Let, $\alpha = 2\cos\frac{2\pi}{5}$, then we have,

$$\begin{aligned}
\alpha^2 + \alpha - 1 &= 4\cos^2\frac{2\pi}{5} + 2\cos\frac{2\pi}{5} - 1 \\
&= 4\sin^2\frac{\pi}{10} + 2\sin\frac{\pi}{10} - 1 \\
&= 4\left(1 - \cos^2\frac{\pi}{10}\right) + 2\sin\frac{\pi}{10} - 1 \\
&= \frac{\cos\frac{\pi}{10}}{\cos\frac{\pi}{10}}\left(4\left(1 - \cos^2\frac{\pi}{10}\right) + 2\sin\frac{\pi}{10} - 1\right) \\
&= \frac{\sin\frac{2\pi}{10} - \cos\frac{3\pi}{10}}{\cos\frac{2\pi}{10}} \\
&= 0
\end{aligned}$$

Now we know, $\alpha = \frac{-1+\sqrt{5}}{2}$ (as $\alpha > 0$) which is constructible.

(ii) **Regular 9-gon is not constractible**. It is equivalent to show $\cos\frac{2\pi}{9}$ is constractible. Since $\cos\frac{2\pi}{3} = -\frac{1}{2}$. We can easily see $\cos\frac{2\pi}{9}$ satisfies the following polynomial,

$$8x^3 - 6x + 1 = 0$$

Which means $2\cos\frac{2\pi}{9}$ satisfy x^3-3x+1. If the above polynomial was redicible over $\mathbb{Q}$ it must have a linear factor. If the cubic polynomial has a rational solution $\frac{p}{q}$ then by rational root theorem, $|p|=1$ and $|q|=1$. we can easily see that ± 1 is not root of the cubic polynomial. So, x^3-3x+1 is irreducible over $\mathbb{Q}$, this means $2\cos\frac{2\pi}{9}$ lies in degree 3 extension over $\mathbb{Q}$ i.e it is not constractible. ■

§ Problem 3

Problem. Decide if the following constructions are possible. If yes, show the methods of construction. If no, state reasons.
(i) Construct a square whose area is equal to that of a given triangle.
(ii) Construct a square whose area is same as the area of a circle of unit radius.
(iii) Construct side length of a cube of volume 2.

Solution. (i) **We can do such construction.** Let ABC is a triangle with $\angle A$ being the largest and hence BCC is the largest side. We can drop a perpendicular AH to BC now the area of $\Delta ABC = \frac{1}{2}BC.AH$. Since BC is already constructed we can construct $\frac{BC}{2}$ and AH is also constructed. So we can construct their product by the method discussed in class. We also can construct a line of length $\sqrt{\frac{1}{2}BC.AH}$, since square root of a constructed number is also constructible.

Construction. Let a triangle ABC be given in the plane. We first construct a rectangle with area equal to that of ABC using the following steps:

i) Construct the line parallel to AB through C. ii) Construct the line perpendicular to AB at A. Let the two lines above intersect at C'. iii) Construct the midpoint M of AC'. iv) Construct the fourth vertex D of the rectangle determined by the vertices A, B, M as the intersection of the perpendicular to AB through B and the line parallel to AB through M. Extend AB to AB' where $|BB'| = |BM|$, by constructing a circle of radius BM centered at B. v) Construct the midpoint of AB' and a circle of radius $\frac{|AB'|}{2}$ centered at this point. vi) Construct the perpendicular to AB' through B, and let it intersect the circle at E. vii) Construct the square $BEFG$ with side length $|BE|$.

(ii) **Such construction is not possible**. If it was possible we can construct $\sqrt{\pi}$ and hence we can construct π and hence π must belong to some finite extension of $\mathbb{Q}$ of degree 2^k but we know, π is not algebraic over $\mathbb{Q}$. Thus, it is not possible.

(ii) **Such construction is not possible**. It's equivalent to construct $\sqrt[3]{2}$. We know the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2 which means $\sqrt[3]{2}$ lies in some degree 3 extension of $\mathbb{Q}$ which is not a power of two. ■

§ Problem 4

Problem. Let C be the field of constractible real numbers. Prove that C is the smallest subfield of $\mathbb{R}$ with the property that if $a \in C$ and $a > 0$, then $\sqrt{a} \in C$.

Proof. We know $\mathbb{Q}$ is constructible, if r_1 is constructible then every elements of $\mathbb{Q}(\sqrt{r_1}) = F_1$ is also constructible, we can continue this arguement and construct fields F_i such that $F_i = F_{i-1}(\sqrt{r_i})$ and all these fields are constructible. By Zorn's lemma there exist a maximal element C such that all element here is constructible. If for any $s \in C$, $\sqrt{s} \notin C$ then, $C(\sqrt{s})$ is the bigger field than C and here all elements are constructible, this contradicts the maximality of C and hence $\sqrt{r} \in C$. Let, F be a subfield of $\mathbb{R}$ which has the property, '$a \in F \Rightarrow \sqrt{a} \in F$'. Since, $\mathbb{Q}$ is prime field $\mathbb{Q} \subset F$, by the construction shows above each F_i are also contained in F and hence by Zorn's lemma C is also contained in F. Thus, C is the minimal with the property, '$a \in F \Rightarrow \sqrt{a} \in F$'. ■

§ Problem 5

Problem. Determine the splitting field of $x^4 + 2$ over $\mathbb{Q}$, and its degree over $\mathbb{Q}$. Is this field same as the splitting field of the polynomial $x^4 - 2$ over $\mathbb{Q}$?

Proof. $x^4 + 2$ is irreducible over $\mathbb{Q}$. If we assume $\sqrt[4]{2}$ is the one root to $x^4 - 2$ in the field $\mathbb{Q}[x]/(x^4 - 2)$,and ζ_8 be the 8-th root of unity, we can see,

$$\left(\sqrt[4]{2}\,\zeta_8^k\right)^4 = -2$$

for $k = 1, 3, 5, 7$. So the splitting field of $x^4 + 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, \zeta_8)$. Now notice that,

$$\left(\sqrt[4]{2}\,i\right)^4 = 2$$

and hence $\mathbb{Q}(\sqrt[4]{2}, i)$ is splitting field of $x^4 - 2$. These fields are isomorphic. If we assume $\mathbb{Q}$ is already contained in $\mathbb{C}$ then we can write,

$$\zeta_8 = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

, thus ζ_8 is already contained in $\mathbb{Q}(\sqrt[4]{2}, i)$ and $i = \zeta_8^2$ thus $i \in \mathbb{Q}(\sqrt[4]{2}, \zeta_8)$ and hence $\mathbb{Q}(\sqrt[4]{2}, \zeta_8) = \mathbb{Q}(\sqrt[4]{2}, i)$. ∎

§ Problem 6

Problem. Find an algebraic closure of the finite field $\mathbb{F}_p$, where p is a prime.

Solution. Recall the construction of $\mathbb{F}_{p^n}$ from $\mathbb{F}_p$. We know $\mathbb{F}_{p^n}$ is a field containing $\mathbb{F}_p$ with $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and is the splitting filed of the polynomial $x^{p^n} - x$. Also $\mathbb{F}_{p^n}$ is unique up-to isomorphism. Now I **claim** that $F = \cup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is algebraic closure of $\mathbb{F}_p$. It is not hard to see F is algebraic over $\mathbb{F}_p$ as any element $\alpha \in F$ must lie in some $\mathbb{F}_{p^n}$ and thus it will satisfy the polynomial $x^{p^n} - x$.

Let, $f(x)$ be a polynomial in $\mathbb{F}_p[x]$, it will split in some field $K = \mathbb{F}_p(\alpha_1, \cdots, \alpha_k)$. Which is a finite extension over $\mathbb{F}_p$. We know any finite extension over $\mathbb{F}_p$ are unique and of the form $\mathbb{F}_{p^j}$, for some $j \in \mathbb{N}$. WLOG we may write $K = \mathbb{F}_{p^\ell}$ is the splitting field of $f(x)$. So, all the root of $f(x)$ lie in $\mathbb{F}_{p^\ell} \subseteq F$. Thus accoding to the definition of algebraic closure in **Dummit-Foote** or class notes, F is algebraic closure of $\mathbb{F}_p$. ∎

§ Problem 7

Problem. Give a proof of the fact that any two algebraic closures of a field are isomorphic. (You may learn a proof, and reproduce it here after understanding.)

Proof. For this we will use the isomorphism extension theorem for any arbitrary collection of polynomials (*Reference*: Fields and Galois Theory- Patrick Morandi).

THEOREM. **(Isomorphism Extension Theorem)** *Let, F, F' be fields and $\sigma : F \to F'$ be an isomorphism. Let, S be a set of polynomial of $F[x]$ with K being the splitting field of polynomials of S. Assume that S' be the set in $F'[x]$, corresponding to the set S i.e $S' = \{\sigma(f) : f \in S\}$, K' be the splitting field of S' over F'. Then σ can be extended to an isomorphism $\tilde{\sigma} : K \to K'$.*

We will use this theorem to prove uniqueness of algebraic closure. If we take $S = F[x]$ then the algebraic closure of F, F_1 is the splitting field for the set S. If F_2 is another algebraic closure of F then, it is also splitting field for the set S. We already have $\text{Id} : F \to F$ an isomorphism, by the above theorem we can extend this to an isomorphic $\sigma : F_1 \to F_2$. Thus algebraic closure of a field is unique up to isomorphism. ∎

§ Problem 8

Problem. Prove that a finite field can never be algebraically closed.

Solution. Let, $a_1, \cdots, a_n$ are elements of a finite field F then the polynomial $f(x) = (x-a_1)\cdots(x-a_n)+a_k$ $(a_k \neq 0)$ do not have any root within the field F. ■

§ Problem 9

Problem. Factor the polynomial $x^{16} - x$ in the fields
(i) $\mathbb{F}_4$
(ii) $\mathbb{F}_8$.

Solution. (i) $\mathbb{F}_{16}$ is the field where $f(x) = x^{16} - x$ splits completely in-fact all elements of $\mathbb{F}_{16}$ are root of the above polynomial. Since $\mathbb{F}_2$ is subfield of $\mathbb{F}_{16}$, it has $0, 1$ as it's root and two more elements of $\mathbb{F}_4$ are roots of the above polynomial. Since $[\mathbb{F}_{16} : \mathbb{F}_4] = 2$, $f(x)$ will have quadratic irreducible factors over $\mathbb{F}_4$. If $t \in \mathbb{F}_4$ and it is non-zero and $\mathbb{F}_4 = \{0, 1, t, t+1 = t^2\}$, we will have $x, (x-1), (x-t), (x-t-1)$ as linear factor. Possible quadratic irreducible factors are, $x^2+x+t, x^2+tx+1, x^2+(t+1)x+1, x^2+x+(t+1), x^2+tx+t, x^2+(t+1)x+(t+1)$. These are irreducible over $\mathbb{F}_4$ as these don't have any root in $\mathbb{F}_4$.

$$x^{16}-x = x(x-1)(x-t)(x-t-1)(x^2+x+t)(x^2+tx+1)(x^2+(t+1)x+1)(x^2+x+(t+1))(x^2+tx+t)(x^2+(t+1)x+(t+1))$$

(ii) $\mathbb{F}_8$ is not an intermediate subfield of $\mathbb{F}_{16}$ and $\mathbb{F}_2$, it also don't contain $\mathbb{F}_4$. No quadratic factor of f in $\mathbb{F}_2$ will get split over $\mathbb{F}_8$, neither any higher degree irreducible terms will get factord in $\mathbb{F}_8$. Thus f over $\mathbb{F}_8$ will have same factorization of $\mathbb{F}_2$. The following fact, *

$$x^{p^n} - x = \prod_{d|n} \prod_{\deg \pi = d} \pi(x)$$

where $\pi(x)$ is irreducible (this is factorization in $\mathbb{F}_p$), will tell us that factorization of f over $\mathbb{F}_2$ will have 2, factor of degree 1,$x, (x-1)$ one factor of degree 2, x^2+x+1 and 3 factor of degree 4, $x^4+x^3+1, x^4+x+1, x^4+x^3+x^2+x+1$, ■

Proof of *: We will prove the following result first. Let $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree d. For $n \geq 0$,

$$f(x) \mid x^{p^n} - x \iff d \mid n$$

If f is irreducible in $\mathbb{F}_p[x]$ of degree d, $\mathbb{F}_p[x]/(f) \cong \mathbb{F}p^d$ and all elements $\alpha \in \mathbb{F}_{p^d}$ satisfy $\alpha^{p^d} = \alpha$. Therefore, $f(x) \mid x^{p^d} - x$ and, by induction, $d \mid n \implies f \mid x^{p^n} - x$. Conversely, assume $f(x) \mid x^{p^n} - x$ and $n = dq + r$ for some $0 < r < d$. As $d \mid dq$ we get $f(x) \mid x^{p^r} - x$. But any $g \in \mathbb{F}_p[x]$ satisfies $g(x^{p^r}) = (g(x))^{p^r}$ and so, $f(x) \mid g(x)^{p^r} - g(x)$ for all $g \in \mathbb{F}_p[x]$. Therefore, the polynomial $t^{p^r} - t$ has all p^d elements of $\mathbb{F}_p[x]/(f)$ as roots and so, $p^d \leq p^r \implies d \leq r$, a contradiction. Hence, $r = 0$ and so $d \mid n$.

Now we will prove the main statement. Let $n \geq 1$. In $\mathbb{F}_p[x]$,

$$x^{p^n} - x = \prod_{d|n} \prod_{\substack{\deg f = d \\ f \text{ monic} \\ \text{irreducible}}} f(x)$$

By the previous lemma, the irreducible factors of $x^{p^n} - x$ in $\mathbb{F}_p[x]$ are exactly the irreducible polynomials whose degree divides n. We now show that no such polynomial appears more than once in the factorization.

Let $f(x) \mid x^{p^n} - x$ for some irreducible $f \in \mathbb{F}_p[x]$. If α is a root of f in a field $F \supset \mathbb{F}_p$, then $\alpha^{p^n} = \alpha$ in F. Therefore, in $F[x]$,

$$\begin{aligned} x^{p^n} - x &= x^{p^n} - x - (\alpha^{p^n} - \alpha) \\ &= (x-\alpha)^{p^n} - (x-\alpha) && (F \text{ has characteristic } p) \\ \implies x^{p^n} - x &= (x-\alpha)((x-\alpha)^{p^n-1} - 1) \end{aligned}$$

As the second factor in the last line above does not vanish at α, α cannot be a multiple root of $x^{p^n} - x$. Hence, $(f(x))^2 \nmid x^{p^n} - x$ and so we are done. □

§ Problem 10

Problem.
Find the splitting field of the polynomial $x^4 + x^2 + 1$ over $\mathbb{Q}$, and its degree over $\mathbb{Q}$.

Solution. Factorizing $x^4 + x^2 + 1$ will give us $(x^2 + x + 1)(x^2 - x + 1)$, let ω be 3-rd root of unity and it is not equal to 1. We can verify ω, ω^2 are root of $x^2 + x + 1$ and $-\omega, -\omega^2$ are root of $x^2 - x + 1$. Thus, the given polynomial splits in the field $\mathbb{Q}(\omega)$. The degree of the extension $\mathbb{Q}(\omega)|_{\mathbb{Q}}$ is 2. ■

§ Problem 11

Problem. Let K be a finite extension of F. Prove that K is a splitting field (of some collection of polynomials) over F iff every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$.

Solution. ($\Rightarrow$) Let, K be a splitting field for $f(x) \in F[x]$ (taking collection of only one polynomial as for finite extension we can consider K as splitting field of finite collection of polynomial. But then taking product of those polynomial will work). Let, $p(x)$ be an irreducible polynomial over F and it has a root $\alpha \in K$. Let, β be a root of $p(x)$. Now, it is clear that $K(\alpha)$ is the splitting field of $f(x)$ over $F(\alpha)$. To see this, note that $f(x)$ splits completely over $K \subseteq K(\alpha)$. Furthermore, suppose L is a field over which $f(x)$ splits completely, and $F(\alpha) \subseteq L \subseteq K(\alpha)$. Then $\alpha \in L$, and since K is the splitting field of $f(x)$ over F, we have $K \subseteq L$. Thus, $K(\alpha) \subseteq L$ and $L = K(\alpha)$ are equal. Likewise, $K(\beta)$ is the splitting field of $f(x)$ over $F(\beta)$. By isomorphism extension theorem, we can get an isomorphism between $K(\alpha)$ and $K(\beta)$. Since, $\alpha \in K$ we can say $K \cong K(\alpha) \cong K(\beta)$, so the degree of extension $K(\beta)|_K$ is one. And hence $\beta \in K$. All roots of $p(x)$ lines in K if one root of $p(x)$ lies in K.

($\Leftarrow$) Let, $K|_F$ is finite extension and every irreducible polynomial with a root in K splits completely. Let, $K = F(\alpha_1, \cdots, \alpha_n)$. Let, $m_i(x)$ be the minimal polynomial of α_i over F. All the minimal polynomial $m_i(x)$ will split completely by the hypothesis. Consider the product, $f(x) = m_1(x) \cdots m_n(x)$. We can see K is splitting field of $f(x)$ over F. ■

§ Problem 12

Problem. Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.

(a) Prove that their composite K_1K_2 is a splitting field over F.

(b) Prove that $K_1 \cap K_2$ is a splitting field over F.

Proof. **(a)** Consider two finite extensions of the field F, denoted as K_1 and K_2, both contained within the larger field K. Let's assume that both K_1 and K_2 are splitting fields over F. Since K_1 is a finite extension, it can be expressed as the splitting field for a finite number of polynomials, specifically, the minimal polynomials of its field generators. By taking the product of these polynomials, we can establish that K_1 is indeed the splitting field for a specific polynomial, denoted as $f_1(x)$. Similarly, K_2 serves as the splitting field for another polynomial, $f_2(x)$.

Now, let's consider the composite field K_1K_2. It's important to note that the polynomial $f_1(x)f_2(x)$ completely factorizes within K_1K_2. Consequently, K_1K_2 contains the splitting field. On the other hand, the splitting field of $f_1(x)f_2(x)$ is generated by the roots of these two polynomials. The roots of $f_1(x)$ are elements of K_1, which is a subset of K_1K_2, and similarly, the roots of $f_2(x)$ are elements of K_2, also a subset of K_1K_2. As a result, the splitting field must be contained within K_1K_2. In conclusion, we can establish that K_1K_2 serves as the splitting field.

(b) Let K_1 and K_2 be finite extensions, both acting as splitting fields over F. Now, consider the field $K_1 \cap K_2$. Our goal is to demonstrate that any irreducible polynomial having a root in $K_1 \cap K_2$ also has all its roots within this same intersection. This proof will establish that $K_1 \cap K_2$ qualifies as a splitting field. Suppose we have an irreducible polynomial $p(x)$ with a root in $K_1 \cap K_2$. This particular root belongs to both K_1 and K_2. However, since K_1 and K_2 are both splitting fields, it follows that all the other roots of $p(x)$ must also reside in K_1 and K_2. Consequently, every root of $p(x)$ is within $K_1 \cap K_2$. As a result of **Problem 11**, we can confirm that $K_1 \cap K_2$ serves as a splitting field. ■

§ Problem 13

Problem. For any prime p and any nonzero $a \in \mathbb{F}_p$ prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$.

Proof. For any element $t \in \mathbb{F}_p$, $t^p - t = 0$ and hence $f(x) = t^p - t + a$ has no root in $\mathbb{F}_p$ as $a \neq 0$. Let, α be a root of t is some extended field $F(\alpha)$, the following calculation shows, $\alpha + j$ is root of $f(x)$ for all $j \in \mathbb{F}_p$.

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^p - (\alpha+1) + a \\ &= \alpha^p + 1 - \alpha - 1 + a \\ &= f(\alpha) = 0 \end{aligned}$$

If f is redicible over $\mathbb{F}_p$ then we can write, $f = gh$ where, $g, h \in \mathbb{F}_p[x]$, so $\alpha + j$ will be roots of g in $F(\alpha)$ for some $j \in \mathbb{F}_p$, hence the sum of roots of g is $(\deg g)\alpha + k$ where, $k \in \mathbb{F}_p$. So, $g(x) = x^{\deg g} - ((\deg g)\alpha + k)x^{\deg g - 1} + \cdots$, but then $(\deg g)\alpha + k \in \mathbb{F}_p$ and hence $\alpha \in \mathbb{F}_p$. ■

§ Problem 14

Problem. Prove that $x^{p^n-1} - 1 = \Pi_{\alpha \in \mathbb{F}_{p^n}^\times}(x - \alpha)$. Derive that the product of the nonzero elements of a finite field is +1 if $p = 2$ and is -1 if p is odd. For p odd and $n = 1$ derive Wilson's theorem: $(p-1)! \equiv -1 (\mathrm{mod} p)$.

Proof. Let, $f(x) = x^{p^n} - x$, and α is a non-zero, non-unit element of $\mathbb{F}_{p^n}$ then, $\alpha^{p^n} - \alpha = 0$ (as $\mathbb{F}_{p^n}$ is a finite field and hence perfect). We can also notice $f(x)$ has roots 0 and 1. Thus we can write,

$$f(x) = \prod_{a \in \mathbb{F}_{p^n}} (x - a)$$

and hence $x^{p^n-1} - 1 = \Pi_{a \in \mathbb{F}_{p^n}^\times}(x - a)$. From here we get $\prod a \in \mathbb{F}_{p^n}^\times a = (-1)^{\left|\mathbb{F}_{p^n}^\times\right| - 1}$, which is 1 is $p = 1$ and -1 if p in odd prime. We know, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, so $1 \cdot 2 \cdots (p-1) = (-1)$ in $\mathbb{Z}/p\mathbb{Z}$, i.e. $(p-1)! \equiv -1 \pmod{p}$ (if p is 2 then $1 = -1$ in $\mathbb{F}_2$). ■