# Interview Questions on Algebra

*Wenhan Dai*

## Set III: Fields and Galois Theory

1. What is the Galois group of a finite field? What is a generator? How many elements does a finite field have? What can you say about the multiplicative group? Prove it.

   *Answer.* Consider $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^r})$ for $r \mid n$ corresponding to an irreducible polynomial of degree $f = n/r$ over $\mathbb{F}_{p^r}$. It is cyclic of order $f$ with generator $\mathrm{Frob}_p$.

   *Claim.* For a finite field $F = \mathbb{F}_{p^d}$, $F^\times = F - \{0\} \cong \mathbb{Z}/(p^d - 1)\mathbb{Z}$ is cyclic.

   *Proof.* Elements of $\mathbb{F}_{p^d}$ are roots of $x^{p^d} - 1$. So each invertible element has a $p$-power order. But $\mathrm{Frob}_p$ acts transitively on these roots, so there is only one generator of $F^\times$ whose order is $p^d - 1$.

   *Warning.* We are morally able to realize $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$. Yet it fails for $\mathbb{F}_{p^d}$.

2. Classify finite fields, their subfields, and their field extensions. What are the automorphisms of a finite field?

   *Answer.* All finite fields are of the form $\mathbb{F}_{p^d}$ with a prime power size. All finite extensions are $\mathbb{F}_{p^m}/\mathbb{F}_{p^d}$ where $d \mid m$. Taking $g$ as the generator of the cyclic group $\mathbb{F}_{p^d}^\times$, then all automorphism $\sigma : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ fixes $g$. This implies that all automorphism are powers of some multiple of $p$.

3. Take a finite field extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. What is Frobenius? What is its characteristic polynomial?

   *Answer.* The Frobenius map is $\mathrm{Frob}(x) = x^p$, which is independent of $n$. Since $\mathbb{F}_{p^n}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$, we have $\mathrm{Frob}^n - 1 = 0$. Note that this extension is of degree $n$, then $X^n - 1$ is the characteristic polynomial.

4. What is the minimal polynomial of the Frobenius automorphism?

   *Answer.* All elements of $\mathbb{F}_{p^n}$ should be zeroes of the minimal polynomial since it is the splitting field. Thus, the minimal polynomial is the same as the characteristic polynomial $X^n - 1$.

5. What's the field with 25 elements?

   *Answer.* It is of the form $\mathbb{F}_5[x]/(\pi(x))$, where $\pi(x)$ is an irreducible polynomial over $\mathbb{F}_5$ of degree 2, such as $\pi(x) = x^2 - 2$, which is irreducible modulo 5 (but it is not because $\pi$ is Eisenstein at 2).

6. What is the multiplicative group of $\mathbb{F}_9$?

   *Answer.* For a finite field $F$, $F^\times = F - \{0\}$. In $\mathbb{F}_9$, it is a cyclic group of order 8.

7. What is a separable extension? Can $\mathbb{Q}$ have a non-separable extension? How about $\mathbb{Z}/p\mathbb{Z}$? Why not? Are all extensions of characteristic 0 fields separable? Of finite fields? Prove it. Give an example of a field extension that's not separable.

   *Note.* Every algebraic extension of a perfect field is automatically separable. Because every minimal polynomial should be irreducible, and hence separable over perfect fields. Recall the definition of perfectness in Question 9.

*Answer.* Say $E/F$ is a separable extension if for all $\alpha \in E$, the minimal polynomial of $\alpha$ over $F$ is separable, i.e. it has no double roots.

Since $\mathbb{Q}$ and $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ are perfect fields, there are no non-separable extensions over them. So do fields of characteristic 0 and finite fields such that $\mathbb{F}_q^p = \mathbb{F}_q$ for $q = p^r$.

*Example.* Consider the non-perfect function field $\mathbb{F}_p(u^p)$ who has an extension $\mathbb{F}_p(u)$. The minimal polynomial of $u$ is $x^p - u^p = (x-u)^p$ since we are working over characteristic $p$. Hence $\mathbb{F}_p(u)/\mathbb{F}_p(u^p)$ is a non-separable extension.

8. Are there separable polynomials of any degree over any field?

   *Answer.* No. Over perfect fields, this should be valid. But for non-perfect fields of characteristic $p$, a polynomial in $x^p$ is always inseparable because it has zero derivative: see, for example, $\mathbb{F}_p(u^p)$, in Question 7.

9. What is a perfect field and why is this important? Give an example of a non-perfect field.

   *Answer.* It is a field such that every irreducible polynomial is separable. A field $F$ is perfect if and only if $\operatorname{char} F = 0$ or $\operatorname{char} F = p$ and $F^p = F$. Equivalently, every finite extension of $F$ is separable. In particular, all finite fields are perfect. The perfect fields are important because all algebraic extensions above them are separable. See this in Question 7.

   *Example.* The function field $\mathbb{F}_p(u)$ is not perfect. Since $x^p - u$ is irreducible (Eisenstein at $u$) but $(x^p-u)' = px^{p-1} = 0$, which is not separable.

10. What is Galois theory? State the main theorem. What are the intermediate extensions? Which extensions are normal, which are not, and why? What are the Galois groups (over $\mathbb{Q}$) of all intermediate extensions?

    *Statement.* Let $K/F$ be a finite Galois extension with $G := \mathrm{Gal}(K/F)$.

    (1) There is a 1-1 correspondence:

    $$\begin{array}{rcl} \{\text{Subgroups } H \geq G\} & \longleftrightarrow & \{\text{Intermediate fields } K/L/F\} \\ H & \longmapsto & K^H = \{x \in K : h(x) = x,\ \forall h \in H\} \\ \mathrm{Gal}(K/L) & \longleftarrow & L. \end{array}$$

    (2) The correspondence is inclusion-reversive:

    $$H_1 \subset H_2 \iff K^{H_1} \supset K^{H_2}, \quad \#H = [K : K^H], \quad [G:H] = [K^H : F].$$

    (3) The correspondence is acted by conjugations: under conjugation,

    $$H \longleftrightarrow L \quad \Longrightarrow \quad gHg^{-1} \longleftrightarrow g(L).$$

    (4) The correspondence is normal-to-normal:

    $$H \lhd G \text{ normal subgroup} \quad \Longleftrightarrow \quad K^H/F \text{ normal extension.}$$

    (5) If $H_1, H_2 \leftrightarrow K_1, K_2$, then

    $$H_1 \cap H_2 \longleftrightarrow K_1K_2; \quad \langle H_1, H_2 \rangle \longleftrightarrow K_1 \cap K_2.$$

11. What is a Galois extension?

    *Definition.* A normal and separable extension, i.e., the splitting field of some polynomial over the base field.

12. Take a quadratic extension of a field of characteristic 0. Is it Galois? Take a degree 2 extension on top of that. Does it have to be Galois over the base field? What statement in group theory can you think of that reflects this?

    *Answer.* The quadratic extension should be Galois whereas the composition of quadratic extensions is not necessarily Galois. A counterexample is $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$.

    The separability is transitive under compositions, but Galois property and normality are not. In group theory, normality is neither transitive: consider

    $$\{(1)\} \triangleleft \mathbb{Z}/2\mathbb{Z} \triangleleft V = (\mathbb{Z}/2\mathbb{Z})^2 \triangleleft A_4 \triangleleft S_4,$$

    where our $\mathbb{Z}/2\mathbb{Z}$ is not normal in $A_4$ or $S_4$.

13. Is abelian Galois extension transitive? That is, if $K$ has abelian Galois group over $E$, $E$ has abelian Galois group over $F$, and $K$ is a Galois extension of $F$, is it necessarily true that $\mathrm{Gal}(K/F)$ is also abelian? Give a counterexample involving number fields as well as one involving function fields.

    *Answer.* No. The upshot is read as the semidirect product of abelian groups is not necessarily abelian.

    *Counterexample.* Over number fields, let's consider

    $$\mathbb{Q} \subset \mathbb{Q}(\omega) \subset \mathbb{Q}(\sqrt[3]{2}, \omega).$$

    One can check $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) = S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is not abelian. Yet its two Galois subgroups are abelian. Since function fields are very similar to number fields, the same construction works:

    $$\mathbb{F}_p(u) \subset \mathbb{F}_{p^2}(u) \subset \mathbb{F}_{p^2}(u^{1/3}).$$

    This tower has the total Galois group $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ as well, which can be non-abelian.

    *Remark.* The compositum in this case is always abelian. It turns out that if $L_1/K$ and $L_2/K$ are Galois over $K$, there exists a natural injective homomorphism

    $$\begin{aligned} \mathrm{Gal}(L_1L_2/K) &\longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\longmapsto (\sigma|_{L_1}, \sigma|_{L_2}). \end{aligned}$$

    In particular, if both $L_1/K$ and $L_2/K$ are abelian, then so is $L_1L_2/K$.

14. Talk about the Kummer extension.

    *Theorem.* (Kummer Theory) For any field $K$, define the Kummer pairing as

    $$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\overline{K}/K) \times K^\times \to \{1, \zeta_n, \ldots, \zeta_n^{n-1}\}.$$

    Then there is an isomorphism induced by the pairing, say

    $$K^\times/(K^\times)^n \simeq \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}).$$

    *Answer.* The Kummer theory can be expressed through a natural language, say the following two types of objects are in the one-to-one correspondence:

(i) Galois extensions of $K$ with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$.

(ii) Subgroups of $K^\times/(K^\times)^n$ that are isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$.

In particular, we suppose $r = 1$. If $\zeta_n \in K$, then every $\mathbb{Z}/n\mathbb{Z}$-extension of $K$ is of the form $K(\alpha^{1/n})$ for some $\alpha \in K^\times$ with the property that $\alpha^{1/d} \notin K$ for any proper divisor $d$ of $n$, and vice versa.

15. Say you have a field extension with only finitely many intermediate fields. Show that it is a simple extension.

*Proof.* Let $L/K$ be such an extension. If $L$ is an algebraic extension, then $L$ is simple by primitive element theorem. Suppose there is a transcendental generator $x \in L$ over $K$. Then $K \subset K(x^n) \subset K(x) \subset L$. When $n$ runs through $\mathbb{N}$, we have infinitely many intermediate fields, which leads to a contradiction.

16. Tell me a condition on the Galois group which is implied by irreducibility of the polynomial. What happens when the polynomial has a root in the base field?

*Answer.* The Galois group is transitive if and only if the polynomial is irreducible. When the polynomial has a root in the base field, the root can be dropped and nothing will happen.

17. What is the discriminant of a polynomial?

*Answer.* By definition, $\operatorname{disc} f = \prod_{i<j}(r_i - r_j)^2$, where $r_1, \dots, r_n$ are all roots of $f$ over its splitting field. Moreover, if $f \in K$ is irreducible of degree $m$, than

$$\operatorname{disc} f = \prod_{1 \le i < j \le n} (r_i - r_j)^2 = (-1)^{m(m-1)/2} \operatorname{Nm}_{L/K} f'(\alpha),$$

where $\alpha$ is a simple root of $f$ in its splitting field $L$.

18. If we think of the Galois group of a polynomial as contained in $S_n$, when is it contained in $A_n$?

*Answer.* This happens for $f \in K[T]$ if and only if $\operatorname{disc} f$ is a square in $K$.

*Proof.* For $\delta = \prod_{i<j}(r_i - r_j)$ and $\sigma \in \operatorname{Gal}(f) = \operatorname{Gal}(K(r_1, \dots, r_n)/K)$, we have

$$\sigma(\delta) = \prod_{i<j}(\sigma(r_i) - \sigma(r_j)) = \varepsilon_\sigma \prod_{i<j}(r_i - r_j) = \varepsilon_\sigma \delta = \pm\delta.$$

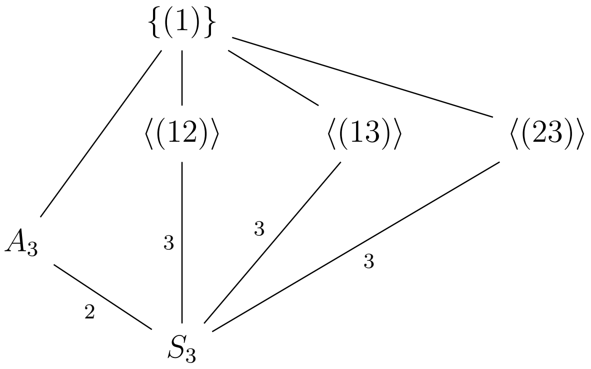
Thus $\sigma \in A_n$ iff $\varepsilon_\sigma = 1$, iff $\sigma(\delta) = \delta$ or $\delta \in K$. This is equivalent to $\operatorname{disc} f = \delta^2 \in K$ is a square in $K$.

19. Is $\mathbb{Q}(\sqrt[3]{2})$ normal? What is its splitting field? What is its Galois group? Draw the lattice of subfields.

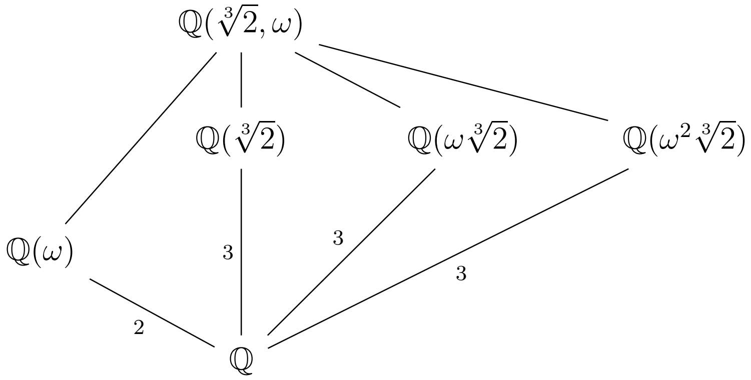
*Answer.* No, the splitting field is $\mathbb{Q}[x]/(x^3 - 2) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. For this,

$$\operatorname{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong A_3 \rtimes \mathbb{Z}/2\mathbb{Z} = S_3.$$

The lattice of subgroups:



This deduces the lattice of subfields:


$\mathbb{Q}(\sqrt[3]{2},\omega)$
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$
$\mathbb{Q}(\omega^2\sqrt[3]{2})$
$\mathbb{Q}(\omega)$
3
3
3
2
$\mathbb{Q}$

20. What is the Galois group of $x^2+1$ over $\mathbb{Q}$? What is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$?

    *Solution.* The splitting field is $\mathbb{Q}(i)$ and the Galois group is $\{1, c\}$, where $c$ is the complex conjugate. Here $d = -1 \equiv 3 \bmod 4$, hence the integral closure of $\mathbb{Z}$ is $\mathbb{Z}[i]$.

21. What's the Galois group of $x^2+9$?

    *Solution.* The splitting field is $\mathbb{Q}(\sqrt{-3})$ with the Galois group $\{1, c\}$.

22. What is the Galois group of $x^2-2$ over $\mathbb{Q}$? Why is $x^2-2$ irreducible?

    *Solution.* The Galois group is $\mathbb{Z}/2\mathbb{Z} \cong \{1, r\}$ where $r$ swaps $\pm\sqrt{2}$, and $x^2-2$ is irreducible over $\mathbb{Q}$ since it is Eisenstein at 2.

23. What is the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$?

    *Solution.* It is $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^2 \cong \{1, r, s, rs\}$ where $r$ swaps $\pm\sqrt{2}$ and $s$ swaps $\pm\sqrt{3}$ (note that $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = 1$ is always trivial). It embeds into $S_4$ by, for example, $\{(1), (12), (34), (12)(34)\}$.

24. What is the Galois group of $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_m})$ over $\mathbb{Q}(\sqrt{n_1} + \ldots + \sqrt{n_m})$?

    *Solution.* It is trivial. May assume all $n_i$ are mutually distinct and square-free. Then each Galois action sends each $\sqrt{n_i}$ to either $\sqrt{n_i}$ or $-\sqrt{n_i}$. Here comes $2^m$ Galois actions. On the other hand, $\sqrt{n_1} + \cdots + \sqrt{n_m}$ also has an orbit of size $2^m$, say $\{\pm\sqrt{n_1} \pm \cdots \pm \sqrt{n_m}\}$. Hence these two fields are equal.

25. What are the Galois groups of irreducible cubics?

    *Answer.* Isomorphic to $A_3$ (otherwise, $S_3$) if $\operatorname{disc} f$ is a square in $K$, where $\operatorname{char} K \neq 2$.

    *Proof.* Just because $\operatorname{Gal}(f) = \operatorname{Gal}(K(r_1, r_2, r_3)/K)$ (being transitive by irreducibility) embeds into $S_3$ and its order is divisible by $[K(r_i) : K] = 3$. So $\operatorname{Gal}(f) = S_3$ or $A_3$. Then apply Question 18.

26. If an irreducible cubic polynomial has Galois group NOT contained in $A_3$, does it necessarily have to be all of $S_3$?

    *Answer.* Yes, for $\operatorname{char} K \neq 2$. See Question 25.

27. Compute the Galois group of $x^3 - 2$ over the rationals.

    *Solution.* Apply Question 25. $x^3 - 2$ is irreducible (Eisenstein at 2) with $\operatorname{disc} = -4a^3 - 27b^2 = -108 \neq \square$ in $\mathbb{Q}$. Hence it is $S_3$.

28. How would you find the Galois group of $x^3 + 2x + 1$? Adjoin a root to $\mathbb{Q}$. Can you say something about the roots of $x^3 + 3x + 1$ in this extension?

    *Solution.* Since $x^3 + 2x + 1$ is irreducible modulo 3, it is irreducible over $\mathbb{Q}$. Note that $\operatorname{disc}(x^3 + 2x + 1) = -59 \neq \square$, it has a Galois group $S_3$.

    *Answer.* The splitting fields of both $x^3 + 2x + 1$ and $x^3 + 3x + 1$ are of degree 6 since both are irreducible polynomials over $\mathbb{Q}$. They are either equal or disjoint. Also, they are equal if and only if their discriminants are differed by some perfect square (i.e. both splitting fields contain the same $\mathbb{Q}(\sqrt{\Delta})$). However, $\operatorname{disc}(x^3 + 3x + 1) = -135$. So none of the roots of $x^3 + 3x + 1$ lie in $\mathbb{Q}[x]/(x^3 + 2x + 1)$.

    *Key Features.* Since the discriminant is a symmetric polynomial of all roots, if $f \in \mathbb{Q}[x]$ is a polynomial with discriminant $\Delta$, then $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}[x]/(f(x))$, containing in the splitting field.

29. Compute the Galois group of $x^3 + 6x + 3$.

    *Solution.* Apply Question 25: $x^3 + 6x + 3$ is irreducible (Eisenstein at 3) with $\operatorname{disc} = -1107 \neq \square$ in $\mathbb{Q}$. Hence it is $S_3$.

30. Find the Galois group of $x^4 - 2$ over $\mathbb{Q}$.

    *Solution.* The splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ with degree 8. And

    $$\operatorname{Gal}(f) \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4.$$

31. What's the Galois group of $x^4 - 3$?

    *Solution.* Similar to Question 30. The answer is $D_4$.

32. What is the Galois group of $x^4 - 2x^2 + 9$?

    *Solution.* This is irreducible over $\mathbb{Q}$ since it is irreducible modulo 5. It has discriminant $186192 = 2^4 \times 3^3 \times 431$ and cubic resolvent $R_3(x) = x^3 - 36x - 4$. Since $R_3(x+1) = x^3 + 3x^2 - 33x - 39$ is Eisenstein at 3, it is irreducible. Hence $\operatorname{Gal}(f) = S_4$ by the following recipe.

    *Recipe.* Here is a general recipe to compute Galois groups of irreducible quartics over $K$ whose characteristics are not 2:

| $\operatorname{disc} f$ in $K$ | $R_3(X)$ in $K[X]$ | $\operatorname{Gal}(f)$ |
|---|---|---|
| $\neq \square$ | irreducible | $S_4$ |
| $= \square$ | irreducible | $A_4$ |
| $\neq \square$ | reducible | $D_4$ or $\mathbb{Z}/4\mathbb{Z}$ |
| $= \square$ | reducible | $V$ |

The cubic resolvent is given by

$$R_3(X) = (X - (r_1r_2 + r_3r_4))(X - (r_1r_3 + r_2r_4))(X - (r_1r_4 + r_2r_3)).$$

In particular, when $f(x) = x^4 + cx + d$, we get $R_3(x) = x^3 - 4dx - c^2$. Also recall that $\operatorname{disc}(x^4 + cx + d) = -27c^4 + 256d^3$.

33. Calculate the Galois group of $x^5 - 2$.

*Solution.* Note that $\mathbb{Q}[x]/(x^5 - 2) = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. Then

$$\operatorname{Gal}(\mathbb{Q}(\zeta_5, \sqrt[5]{2})/\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/4\mathbb{Z},$$

where $\varphi : \mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$ is nontrivial but unique.

34. Discuss sufficient conditions on a polynomial of degree 5 to have Galois group $S_5$ over $\mathbb{Q}$ and prove your statements.

*Answer.* The sufficient conditions can be various. We let the irreducible polynomial have exactly 3 real roots and a pair of complex roots. By labeling these roots $\{1, 2, 3, 4, 5\}$, our condition leads to the existence of a transposition and a 3-cycle in Galois group. However, a transitive subgroup of $S_n$ that contains a transposition and a $p$-cycle with $p > n/2$ can only be $S_n$ itself.

35. Show that if $f$ is an irreducible quintic with precisely two nonreal roots, then its Galois group is $S_5$.

*Proof.* In the conclusion of Question 23 of Set I, we see $S_n$ can be generated by $(a\ b)$ and $(1\ 2 \cdots n)$ if $(b - a, n) = 1$. In this case, as $f$ has a couple of conjugate complex roots, there exists some prime $p$ such that $f(x) \equiv f_3(x)f_2(x) \bmod p$, where $\deg f_2 = 2$ is irreducible over $\mathbb{F}_p$ and $\deg f_3 = 3$. Then (possibly after permuting the roots of $f$ when necessary), $\operatorname{Gal}(f)$ contains $(1\ 2\ 3)$ and $(4\ 5)$. Consequently, $\operatorname{Gal}(f) = S_5$.

36. Suppose you have a degree 5 polynomial over a field. What are necessary and sufficient conditions for its Galois group to be of order divisible by 3? Can you give an example of an irreducible polynomial in which this is not the case?

*Answer.* The Galois group has order divisible by 3 if and only if it contains an element of order 3, namely a 3-cycle. Equivalently, there is some prime $p$ such that $f(x) \bmod p$ has an irreducible factor of degree 3.

*Example.* Let $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$. Then $\operatorname{Gal}(f) \cong D_5$ if and only if:

(i) $f(x)$ is irreducible over $\mathbb{Q}$;

(ii) $\operatorname{disc}(f(x)) = 4^4a^5 + 5^5b^4 = \square$ is a perfect square;

(iii) $f(x)$ is solvable by radicals.

37. What is the Galois group of $x^7 - 1$ over the rationals?

*Solution.* See Question 38 below. It's $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.

38. What is the Galois group of the polynomial $x^n - 1$ over $\mathbb{Q}$?

*Answer.* We have $\mathbb{Q}[x]/(x^n - 1) = \mathbb{Q}(\zeta_n)$ and an isomorphism

$$\begin{aligned}(\mathbb{Z}/n\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\\ k \bmod n &\longmapsto \sigma_k,\end{aligned}$$

where $\sigma_k(x) = x^k$.

39. Describe the Galois theory of cyclotomic extensions.

*Answer.* Same as Question 38. Note that one can use Kronecker–Weber theorem to determine the abelian extension (in explicit description) for a given cyclic Galois group.

40. What is the maximal real field in a cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$?

*Answer.* It's $M = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Since $\mathbb{Q}(\zeta_n)$ is not totally real, we have $[\mathbb{Q}(\zeta_n) : M] \geq 2$. This morally equal to 2: convert $\mathbb{Z}/2\mathbb{Z}$ into a multiplicative group $\{\pm 1\}$, which fixes

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/M}(\zeta_n) = \zeta_n + \zeta_n^{-1}.$$

*Remark.* The intrinsic fact we've used here is $\varphi(n)$ being even for all $n \geq 3$.

41. Compute the Galois group of $p(x) = x^7 - 3$.

*Answer.* The splitting field is $\mathbb{Q}(\sqrt[7]{3}, \zeta_7)$. Hence

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{3}, \zeta_7)/\mathbb{Q}) = \mathbb{Z}/7\mathbb{Z} \rtimes_\varphi \mathbb{Z}/6\mathbb{Z},$$

where $\varphi : \mathbb{Z}/6\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ is nontrivial but unique.

42. What Galois stuff can you say about $x^{2^n} - 2$?

*Answer.* Recall that

$$\mathrm{disc}(x^k + a) = (-1)^{k(k-1)/2} k^k a^{k-1}.$$

Then $\mathrm{disc}(x^{2^n} - 2) = -2^{(n+1)\cdot 2^n} \neq \Box$ for any $n \geq 2$. The splitting field is $\mathbb{Q}(\zeta_{2^n}, 2^{2^{-n}})$, and the Galois group is $\mathbb{Z}/2^n\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z})$ when $n > 2$.

43. What are the cyclic extensions of (prime) order $p$?

*Answer.* By Kronecker–Weber, it is a subfield $F$ of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ for some integer $n$ such that $p \mid \varphi(n)$. Say $\varphi(n) = kp$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(n)\mathbb{Z}$ who has a subgroup $\mathbb{Z}/k\mathbb{Z} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/F)$. This subgroup has image $\langle x \rangle \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $x^k = 1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ under multiplication. Then

$$F = \mathbb{Q}(\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/F}(\zeta_n)) = \mathbb{Q}(\zeta_n + \zeta_n^x + \cdots + \zeta_n^{x^{k-1}}).$$

*Caution.* This question is not asking for cyclotomic extensions $\mathbb{Q}(\zeta_p)$. But recall that $\mathbb{Q}(\zeta_p)$ is the smallest extension generated by Kronecker–Weber that contains $\mathbb{Q}(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$; namely, $p$ is the conductor of $\mathbb{Q}(\sqrt{p^*})$. This fact relates to the quadratic reciprocity.

44. Can you give me a polynomial whose Galois group is $\mathbb{Z}/3\mathbb{Z}$?

    *Answer.* Any irreducible cubic whose discriminant is a square. For example, $x^3-3x-1$ with disc $= 81$, whose roots are $r, r^2-r-2, -r^2+2$.

45. Which groups of order 4 can be realised as a Galois group over $\mathbb{Q}$?

    *Answer.* Both of them: for square-free integers $m \neq n$,

    $$\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}, \quad \mathrm{Gal}(\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

46. Give a polynomial with $S_3$ as its Galois group.

    *Answer.* It must be an irreducible cubic whose discriminant is not a rational square.

47. How do you construct a polynomial over $\mathbb{Q}$ whose Galois group is $S_n$? Do it for $n = 7$ in particular.

    *Key Tool.* For $n \geq 2$, let $H$ be a transitive subgroup of $S_n$. If one of the followings are valid, then $H = S_n$:

    - $H$ contains a 2-cycle (i.e., a transposition) and a $p$-cycle ($p > n/2$),
    - $H$ contains a 2-cycle and a $(n-1)$-cycle, or
    - $n \geq 3$, $H \neq A_n$ contains a 3-cycle and a $p$-cycle ($p > n/2$).

    *Answer.* We need to consider an irreducible polynomial of degree 7 who has a degree-2-factor mod $p$ together with a degree-6-factor mod $q$ for some primes $p, q$. Let $f(X) = X^7 - X - 1$. The first few factorizations of $f(X)$ mod $p$ are as follows:

    $$\begin{aligned} f(X) &\equiv X^7 + X + 1 \bmod 2, \\ f(X) &\equiv (X^2 + X + 2)(X^5 + 2X^4 + 2X^3 + 2X + 1) \bmod 3, \\ f(X) &\equiv (X + 3)(X^6 + 2X^5 + 4X^4 + 3X^3 + X^2 + 2) \bmod 5. \end{aligned}$$

    So $f(X)$ is in need.

48. What's a Galois group that's not $S_n$ or $A_n$?

    *Answer.* It's in general a composition of series of semidirect products of cyclic groups. A quartic extension may have Galois group $V = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $D_4 = \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

49. Which finite groups are Galois groups for some field extension?

    *Answer.* The following theorem by Artin shows that each finite group can be realized as a Galois group: given a field $K$ and let $G \leq \mathrm{Aut}(K)$; then $K/K^G$ is a Galois extension with Galois group $G$.

    Under this assumption, let $F$ be an arbitrary field and adjoin all $g \in G$ as transcendental elements into $F$ to get $L = F(g_1, \ldots g_n)$, where $n = |G|$. Note that any action of $G$ on $L$ gives a multiplication over generators, so $G$ embeds into $\mathrm{Aut}(L)$. This shows that $\mathrm{Gal}(L/L^G) = G$.

50. What Galois group would you expect a cubic to have?

    *Answer.* Suppose the cubic is irreducible and then the Galois group is transitive. Since we get an intermediate field by adding only one root, the Galois group is a subgroup with order divisible by 3. Hence it's $A_3$ or $S_3$.

51. Draw the subgroup lattice for $S_3$.

    *Answer.* There are 3 subgroups of index 3; only $A_3$ has index 2. See Question 19.

52. Do you know what the quaternion group is? How many elements are there of each order? Suppose I have a field extension of the rationals with Galois group the quaternion group. How many quadratic extensions does it contain? Can any of them be imaginary?

    *Answer.* For the quaternion group, see Question 27 in Set I. There are 3 different quadratic extensions, say $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$, and $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Note that at least one of them is totally real.

    A theorem of Witt asserts that a biquadratic extension $F(\sqrt{a}, \sqrt{b}), a, b \in F^\times$ can be embedded in a quaternion Galois extension of $F$ iff the quadratic form $ax^2+by^2+abz^2$ is isomorphic over $F$ to $x^2 + y^2 + z^2$. For $F = \mathbb{Q}$ this forces $a, b, ab > 0$. Hence all of them cannot be imaginary.

53. Suppose you are given a finite Galois extension $K/\mathbb{Q}$ by $f(x) \in \mathbb{Z}[x]$ such that $\deg(f) = n$ and $\mathrm{Gal}(K/\mathbb{Q}) = S_n$. What can you say about the roots?

    *Answer.* Since $S_n$ acts transitively on roots of $f$ over $K$, $f$ must be irreducible over $\mathbb{Q}$. The Galois group contains permutations of length $2 \leq \ell \leq n$, hence $f$ contains irreducible factors of degree $2 \leq d \leq n$ for different primes. The roots of $f$ must be independent in the sense of additive linear combinations and multiplicative power combinations.

54. How many automorphisms does the complex field have? How can you extend a simple automorphism (e.g. $\sqrt{2} \mapsto -\sqrt{2}$) of an algebraic field into $\mathbb{C}$? How can you extend a general subfield isomorphism? What feature of $\mathbb{C}$ allows you to?

    *Answer.* There are only two continuous automorphisms on $\mathbb{C}$ that is compatible with the topology. If we drop the topology, there must be infinitely ($2^{\aleph_0}$-uncountably) many of them.

    It is not true that any isomorphism between subfields of $\mathbb{C}$ can be extended to $\mathbb{C}$. See Question 55 below for a counterexample. However, one can always extend it to some subfield that is isomorphic to $\mathbb{C}$. Given an isomorphism $K \to L$ of number fields in $\mathbb{C}$. Then $K \otimes_{\mathbb{Q}} \mathbb{Q}_p \to L \otimes_{\mathbb{Q}} \mathbb{Q}_p$ for some $p$ is naturally constructed, and can be extended to $\overline{\mathbb{Q}_p}$. Indeed, one can fix some $\overline{\mathbb{Q}_p} \cong \mathbb{C}$ to translate this argument onto $\mathbb{C}$.

    *Remark.* The feature of $\mathbb{C}$ we have used here is that any algebraic closure of any subfield (especially, local subfield) of $\mathbb{C}$ is contained in $\mathbb{C}$. Hence we can construct isomorphisms to $\mathbb{C}$ such as $\overline{\mathbb{Q}_p} \cong \mathbb{C}$.

55. Can it happen that a proper subfield of $\mathbb{C}$ is isomorphic to $\mathbb{C}$? How?

    *Answer.* Yes. Choose a countable set of elements of $\mathbb{C}$ (not necessarily transcendental over $\mathbb{Q}$), say $\{\alpha_n\}_{n\in\mathbb{N}}$. Consider $\sigma \in \mathrm{Aut}(\mathbb{Q}(\alpha_0, \alpha_1, \cdots))$ such that $\sigma(\alpha_i) = \alpha_{i+1}$. Apply Zorn's lemma to

    $$\mathfrak{F} = \{\widetilde{\sigma} \text{ extension of } \sigma \text{ to } \mathbb{C} : \alpha_0 \notin \operatorname{im} \widetilde{\sigma}\},$$

    and we get a maximal element (in the sense of restriction) $f \in \mathfrak{F}$, whose image is isomorphic to $\mathbb{C}$ such that $\alpha_0 \in \mathbb{C} - f(\mathbb{C})$.

56. Consider the minimal polynomial $f(x)$ for a primitive $m$-th root of unity. Prove that if $p$ divides $f(a)$ for some integer $a$ and $(p,m)=1$, then $m$ divides $p-1$. Use this fact to show that there are infinitely many primes congruent to 1 mod $m$.

    *Proof.* By assumption $a$ is the image of $\zeta_m$ in $\mathbb{F}_p$. Then $a^m = 1$ from $(p,m)=1$. Since $\zeta$ is the primitive root, we see $a$ has order $m$. On the other hand, by Fermat's little theorem, since $a \neq 0$, we have $a^{p-1}=1$, which shows that $m \mid (p-1)$. By varying the choice of $a$ with $m$ fixed, $f(a)$ can have infinitely many possible prime divisors. Since there are only finitely many $p$ such that $(p,m)=p$, we have infinitely many $p$ such that $m \mid (p-1)$, namely $p \equiv 1 \bmod m$.

57. What is Dirichlet's theorem about primes in arithmetic progression? What can you say about the density of such primes?

    *Statement.* (Dirichlet) Given coprime integers $a, m$, there are infinitely many primes $p$ such that $p \equiv a \bmod m$. Namely, there are infinitely many primes lies in a fixed arithmetic progress.

    *Theorem.* (Chebotarev) Let $E/F$ be a Galois (not necessarily finite) extension, then

    $$\delta\{p \in \mathcal{O}_F \text{ prime} : p \nmid \mathrm{disc}_{E/F}, \mathrm{Frob}_p \in C\} = \frac{\#C}{\#\,\mathrm{Gal}(E/F)}.$$

    Namely, the density of some unramified primes whose Frobenius maps form a conjugacy class $C$ in $\mathrm{Gal}(E/F)$ equals to the proportion of $C$ in $\mathrm{Gal}(E/F)$.

    *Application.* It turns out that $\delta\{p \in \mathbb{Z} \text{ is prime} : p \equiv a \bmod m\} = 1/\varphi(m) \neq 0$, hence these primes are infinitely many: consider the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for which

    $$G := \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

    Here we get an abelian cyclic group whose conjugacy classes are given by single elements. Since $(a,m)=1$, we have

    $$\begin{aligned} \mathbb{Z}/\varphi(m)\mathbb{Z} &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a \bmod m &\longmapsto (\zeta_m \mapsto \zeta_m^a). \end{aligned}$$

    Hence the conjugacy class $C = \{\mathrm{Frob}_a\}$, and the density is $\#C/\#G = 1/\varphi(m)$.

58. How many irreducible polynomials of degree six are there over $\mathbb{F}_2$?

    *Solution.* The splitting field of any irreducible polynomial of degree 6 over $\mathbb{F}_2$ is $\mathbb{F}_{2^6}$. The root system is generated by $\alpha \in \mathbb{F}_{2^6} - (\mathbb{F}_{2^2} \cup \mathbb{F}_{2^3})$. Any Galois action is given by $\mathrm{Frob}_2$ as a permutation on roots. Note that $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^3} = \mathbb{F}_2$ and those irreducible polynomials must be monic over $\mathbb{F}_2$, hence

    $$\frac{2^6 - 2^3 - 2^2 + 2}{6} = 9$$

    counts the number as desired.

59. Can you have a degree 7 irreducible polynomial over $\mathbb{F}_p$? How about a degree 14 irreducible polynomial?

    *Solution.* Over $\mathbb{F}_p$, there are $(p-1)(p^7-p)/7$ irreducible polynomials of degree 7, and $(p-1)(p^{14}-p^7-p^2+p)/14$ irreducible polynomials of degree 14. For the reason, see Question 58.

60. How many irreducible polynomials are there of degree 4 over $\mathbb{F}_2$?

    *Solution.* The number is $(2^4 - 2^2)/4 = 3$. In an explicit description, they must have constant item 1 with odd number of monomials:

    $$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1.$$

    Here $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ is not irreducible.

61. For each prime $p$, give a polynomial of degree $p$ that is irreducible over $\mathbb{F}_p$. You can do it in a "uniform" way.

    *Construction.* The answer is $x^p - x - 1$. This polynomial, which is irreducible modulo $p$, must be a factor of $x^{p^p} - 1$. It is because an irreducible polynomial of degree $p$ has splitting field $\mathbb{F}_{p^p}/\mathbb{F}_p$, and $x^{p^p} - 1$ runs through all elements of $\mathbb{F}_{p^p}$ as its roots. On the other hand, by Fermat's little theorem, $x^p - x - 1$ has value $-1$ for all $x \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

62. Can we solve general quadratic equations by radicals? And what about cubic and so on? Why can't you solve 5-th degree equations by radicals?

    *Proposition.* Over a characteristic 0 field, a polynomial is radically solvable if and only if the Galois group of its splitting field is solvable.

    *Answer.* General quartic, cubic, and quadratic equations are all radically solvable. However, neither $A_5$ nor $S_5$ are solvable groups.

63. Talk about solvability by radicals. Why is $S_5$ not solvable? Why is $A_5$ simple?

    *Answer.* See Question 62 above. Since $A_5$ is simple and has no normal subgroups, there will never be such an ascending sequence whose subquotients $G_j/G_{j-1}$ are abelian. So $S_5$ is not solvable.

    *Proof idea.* To show that $A_5$ is simple, one way is by considering the sizes of its conjugacy classes. Another way is by using a fact that for $n \geqslant 5$, every nontrivial conjugacy class in $A_n$ contains at least $n$ elements (c.f. Set I, Question 21).

64. For which $n$ can a regular $n$-gon be constructed by ruler and compass?

    *Answer.* A regular $n$-gon is constructible if and only if $\alpha = \cos(\frac{2\pi}{n})$ is constructible, which is equivalent to $[\mathbb{Q}(\alpha), \mathbb{Q}]$ is a power of 2. It turns out to be $n = 2^k p_1 \cdots p_t$, where $p_i = 2^{2^{n_i}} + 1$ are Fermat primes.

65. How do you use Galois theory (or just field theory) to prove the impossibility of trisecting an angle? Doubling a cube? Squaring a circle?

    *Recipe.* Saying "constructible" means the ratio of volumes, the cosine or sine of angles, etc. are all constructible. A number $\alpha$ is said to be constructible if $\alpha$ lies in the top of a finite tower of real quadratic extensions starting from $\mathbb{Q}$.

    *Proof.* **Trisecting an angle:** over the number field $K = \mathbb{Q}(\cos\theta)$, the tripled cosine equality $\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$ shows that $[K(\cos(\theta/3)) : K] = 3$.

    **Doubling a cube:** this requires $\sqrt[3]{2}$ to be constructible; but $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

    **Squaring a circle:** this requires $\sqrt{\pi}$ to be constructible, and hence $\pi$ is constructible; but the contradiction lies in that $\pi$ is transcendental over $\mathbb{Q}$.

66. Which numbers are constructible? Give an example of a non-constructible number whose degree is nevertheless a power of 2.

    *Answer.* See Question 65 above.

67. State and prove Eisenstein's Criterion.

    *Statement.* Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If there is a prime $p$ such that $p \mid a_{n-1}, \ldots, a_0$ but $p \nmid a_n$, $p^2 \nmid a_0$, then $f$ is irreducible over $\mathbb{Z}$.

    *Proof.* Suppose $f = gh$ in $\mathbb{Z}[x]$. Since $f \equiv a_n x^n \bmod p$ and $\mathbb{F}_p[x]$ is a UFD, we get $g \equiv b_i x^i \bmod p$ and $h \equiv c_j x^j \bmod p$ for $i + j = n$. So the constant terms of $g, h$ over $\mathbb{Z}$ are divisible by $p$, hence $p^2 \mid a_0$, a contradiction.

68. Why is $(x^p - 1)/(x - 1)$ irreducible over $\mathbb{Q}$?

    *Proof.* It's because $f(x + 1)$ is Eisenstein at $p$.

69. Can you prove the fundamental theorem of algebra using Galois theory? What do you need from analysis to do so?

    *Galois-theoretic Proof.* We have to show any $f(x) \in \mathbb{R}[x]$ has a root in $\mathbb{C} = \mathbb{R}[i]$. Suppose $f(x) \neq x^2 + 1$ is monic and irreducible. Note that when $2 \nmid \deg f(x)$, there is a real root of $f(x)$. (This is the key feature of $\mathbb{R}$ that depends only on the Mean Value Theorem.) Let $E$ be the splitting field of $(x^2 + 1)f(x)$. But one can show that $E = \mathbb{C}$.

    *Details.* Note that $E \supset \mathbb{C}$ and we aim to show the equality. Since $\mathbb{R}$ has characteristic 0, $(x^2 + 1)f(x)$ is separable, and so $E$ is Galois over $\mathbb{R}$. Since $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, there exists a Sylow 2-subgroup of $\mathrm{Gal}(E/\mathbb{R})$, say $H$. Consider $\mathbb{R} \subset M = E^H \subset E$. We obtain $[M : \mathbb{R}] = [G : H]$ by Galois theory. On the other hand, $2 \nmid [G : H]$ by Sylow's theorems. So for each $\alpha \in M$, its minimal polynomial is of an odd degree, and obtains a real root. It forces $\alpha \in \mathbb{R}$, and hence $M = \mathbb{R}$ with $G = H$. It follows that $|\mathrm{Gal}(E/\mathbb{C})| = 2^r$ for some $r \geqslant 0$. If $r > 0$ then $\mathrm{Gal}(E/\mathbb{C})$ has a subgroup $N$ of index 2, and $[E^N : \mathbb{C}] = 2$. So $E^N$ is generated by square roots of elements in $\mathbb{C}$, which is again lying in $\mathbb{C}$. Thus $E^N = \mathbb{C}$ and $r = 0$. We accomplish the proof that $E = \mathbb{C}$.

    *Analytic Proof.* We can use real differential calculus involving the Extreme Value Theorem for real-valued functions of two real variables. Alternatively, let $f : \mathbb{C} \to \mathbb{C}$ be any polynomial, then there exists $z_0 \in \mathbb{C}$ where $|f(z)|$ attains its minimum in $\mathbb{R}$.

70. What are the symmetric polynomials?

    *Answer.* Those are unchanged if their variables are arbitrarily permuted.

71. State the fundamental theorem of symmetric polynomials.

    *Statement.* Any symmetric polynomial can be expressed into a polynomial (over the base field) of elementary symmetric polynomials.

72. Is the discriminant of a polynomial always a polynomial in the coefficients? What does this have to do with symmetric polynomials?

    *Answer.* Yes. The discriminant is a symmetric polynomial in all roots, and hence a polynomial of elementary symmetric ones. But the elementary ones are coefficients. Here we have used the the fundamental theorem of symmetric polynomials.

73. Find a non-symmetric polynomial whose square is symmetric.

    *Solution.* For example, the root of the discriminant.

74. Let $f$ be a degree 4 polynomial with integer coefficients. What's the smallest finite field in which $f$ necessarily has four roots?

    *Solution.* Consider $\overline{f} \in \mathbb{F}_p[x]$. If it is irreducible of degree 4, then $\mathbb{F}_{p^4}$ contains all of its roots. The smallest one (with respect to the size) can be $\mathbb{F}_{16}$.

75. Define $p$-adic numbers. What is a valuation?

    *Definition.* For a fixed prime $p$, the most usual definition is to say $p$-adic number $\mathbb{Q}_p$ is the topological completion of $\mathbb{Q}$ with respect to the non-archimedean absolute value $|\cdot|_p := (1/p)^{\mathrm{ord}_p(\cdot)}$.

    *Remark.* By Ostrowski's theorem, any nontrivial non-archimedean absolute value on $\mathbb{Q}$ is equivalent to (i.e. is some integral power of) the $p$-adic valuation for some prime $p$. Also, any nontrivial archimedean absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$.

    *Answer.* A valuation is a surjective homomorphism $v : K^\times \to \mathbb{Z}$ defined over a field $K$. It is often taken as a logarithm of some $|\cdot|$.

76. What's Hilbert's theorem 90?

    *Theorem.* (Hilbert 90) Suppose $G$ is a (Galois) group and $M$ is an abelian group equipped with a $G$-action. Then define the first order **group cohomology** by

    $$H^1(G, M) := \frac{\{f : G \to M \text{ such that } f(gh) = f(g)^h f(h) \text{ for all } g, h \in G\}}{\{f : G \to M \text{ such that } f(g) = x(x^g)^{-1} \text{ for some } x \in M\}}.$$

    If $L/K$ be a finite Galois extension with Galois group $G$. Then $H^1(G, L^\times) = 0$.

77. Consider a nonconstant function between two compact Riemann Surfaces. How is it related to Galois theory and algebraic number theory?

    *Answer.* Let $X$ and $Y$ be compact connected Riemann surfaces, and let $\alpha : Y \to X$ be a nonconstant holomorphic mapping. Write $\mathcal{M}(X)$ and $\mathcal{M}(Y)$ for the fields of meromorphic functions on $X$ and $Y$. The map $f \mapsto f \circ \alpha$ is an inclusion $\mathcal{M}(X) \hookrightarrow \mathcal{M}(Y)$ which makes $\mathcal{M}(Y)$ into a field of finite degree over $\mathcal{M}(X)$; let $m$ be this degree. Geometrically, the map is $m$-to-1 except at a finite number of branch points.

    Let $P \in X$ and let $\mathcal{O}_P$ be the set of meromorphic functions on $X$ that are holomorphic at $P$ — it is the discrete valuation ring attached to the discrete valuation $\mathrm{ord}_P$, and its maximal ideal $\mathfrak{p}$ is the set of meromorphic functions on $X$ that are zero at $P$. Let $B$ be the integral closure of $\mathcal{O}_P$ in $\mathcal{M}(Y)$. Let $\alpha^{-1}(P) = \{Q_1, \ldots, Q_g\}$ and let $e_i$ be the number of sheets of $Y$ over $X$ that coincide at $Q_i$. Then $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$, where $\mathfrak{q}_i$ is the prime ideal $\{f \in B \mid f(Q_i) = 0\}$.