Instructional School for Teachers

Fields and Algebraic Number Theory

June 04-16, 2018

(IIT Mandi)

Dr. Amit Kulshrestha from IISER Mohali delivered six lecture of 90 minutes each on Field Theory. During these lectures he covered the following topics.

1. Field extensions, algebraic extensions.
2. Group of automorphisms and fixed fields.
3. Splitting fields, normal extensions, algebraic closure.
4. Separable extensions, perfect fields.

5. Galois extensions and Galois group.

6. Fundamental theorem of Galois theory.

In the beginning of this lecture series participants were made to realize that the if for a field extension K/F the base field F equals to fixed field of the group $\mathrm{Gal}(K/F)$ of F-automorphisms of K then extension possesses some special properties. Thereafter, concepts of normal extensions and separable extensions were decuced as natural conditions in order to achieve $F = \mathcal{F}(\mathrm{Gal}(K/F))$, where $\mathcal{F}(S)$ denotes the fixed field of a set S of automorphisms of K.

These lectures were helpful for participants in building their basics of number fields. Tutorial sessions of six hours were conducted to discuss the following problems based on these lectures.

1. Are $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ isomorphic as vector spaces over $\mathbb{Q}$? Are they isomorphic as fields?

2. Let K be a field such that $\mathbb{F}_p \subseteq K$ and $n = [K : \mathbb{F}_p] < \infty$. Show that K is finite. How many elements are there in K?

3. Show that the set $F((x)) := \left\{ \sum_{i=n}^{\infty} a_i x^i : n \in \mathbb{Z}, a_i \in F \right\}$ of formal power series equipped with degree-wise addition of coefficients and the multiplication defined by
$$\left(\sum_{i=n}^{\infty} a_i x^i \right) \left(\sum_{j=m}^{\infty} b_j x^j \right) = \sum_{k=n+m}^{\infty} \left(\sum_{\ell=n}^{k-m} a_\ell b_{k-\ell} \right) x^k$$
is a field.

4. Show that if $f(x) \in \mathbb{Q}[x]$ is a reducible polynomial then the quotient $\mathbb{Q}[x]/\langle f(x) \rangle$ is not a field, where $\langle f(x) \rangle$ denotes the principal ideal of $\mathbb{Q}[x]$ generated by $f(x)$.

5. Let K be an extension of F and $X \subseteq K$. If $F(X)$ denotes the intersection of all subfields of K that contain both F and X then show that $F(X)$ is a field.

6. Let K be an extension of F. Let $\alpha \in K$ be an algebraic element over F. Show that there exists a unique irreducible monic polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.

7. Consider the subfields $L_1 = \mathbb{Q}(\sqrt{2})$ and $L_2 = \mathbb{Q}(\sqrt{3})$ of $\mathbb{R}$. Show that the compositum $L_1 L_2$ equals $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. What is the degree $[L_1 L_2 : \mathbb{Q}]$?

8. Let both L/F and K/L be algebraic extensions. Show that K/F is also algebraic.
(Hint : Let $\alpha \in K$, with the minimal polynomial $\min(L, \alpha) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Take $L_0 = F(a_0, a_1, \cdots, a_{n-1})$. Show that $[F(\alpha) : F] \leq [L_0(\alpha) : F] < \infty$. How do we argue further?)

9. Let K/F be a field extension such that $[K : F]$ is prime. Show that there is no field L such that $F \subsetneq L \subsetneq K$. Give examples of such extensions. What is your opinion about the converse of it?

10. Show that $\mathrm{Gal}(\mathbb{F}_2(x)/\mathbb{F}_2(x^2))$ is trivial. Can you generalise it for the fields of characteristic $p \neq 0$?

11. Let K be a field and $\mathrm{Aut}(K)$ be the group of all automorphisms of K. For a subset $S \subseteq \mathrm{Aut}(K)$, define $\mathcal{F}(S) := \{a \in K : \varphi(a) = a \text{ for all } \varphi \in S\}$ and for a subfield $L \subseteq F$ define $\mathrm{Gal}(K/L) := \{\varphi \in \mathrm{Aut}(K) : \varphi(a) = a \text{ for all } a \in L\}$. Convince yourself that the following are true.

    (a) If $S \subseteq \mathrm{Aut}(K)$ then $\mathcal{F}(S) = \mathcal{F}(\mathrm{Gal}(K/\mathcal{F}(S))$.

    (b) If L is a subfield of K then $\mathrm{Gal}(K/L) = \mathrm{Gal}(K/\mathcal{F}(\mathrm{Gal}(K/L))$.

12. Show that $\mathrm{Aut}(\mathbb{R})$ is finite while $\mathrm{Aut}(\mathbb{C})$ is infinite. What is $|\mathrm{Aut}(\mathbb{R})|$?

13. Let ω denote a complex cube root of 1 and $\alpha = 2^{\frac{1}{3}} \in \mathbb{R}$ be the real cube root of $x^3 - 2 = 0$.

    (a) Show that the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois. Find $|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})|$.

    (b) Show that the extension $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ is Galois. Find $|\mathrm{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})|$.

14. Show that $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ is an irreducible polynomial. Let α be a root of $f(x)$. Show that $\varphi : \mathbb{F}_2(\alpha) \to \mathbb{F}_2(\alpha)$ defined by $\varphi(a + b\alpha) = a + b + b\alpha$, where $a, b \in \mathbb{F}_2$, is an $\mathbb{F}_2$-automorphism of $\mathbb{F}_2(\alpha)$. Determine $\mathrm{Gal}(\mathbb{F}_2(\alpha)/\mathbb{F}_2)$. Is $\mathbb{F}_2(\alpha)/\mathbb{F}_2$ Galois?

15. Let $K = F(x)$, the field of rational functions in one variable over F. Let automorphisms $\varphi : K \to K$ and $\psi : K \to K$ be determined, respectively, by $\varphi(x) = 1/x$ and $\psi(x) = 1 - x$. Let $S := \{\varphi, \psi\}$. Find $\mathcal{F}(S)$.

16. Let K be a field and V denote the set of all (set theoretic) functions $f : K^* \to K$. One equips V with a vector space structure via pointwise addition of functions and natural multiplication of scalars in K with elements in V. Show that $\mathrm{Aut}(K)$ is a linearly independent set in V.

17. Determine if the extension $\mathbb{Q}(\sqrt{5} + \sqrt{7})$ is Galois over $\mathbb{Q}$.

18. Let $S = \{f_1(x), f_2(x), \cdots, f_n(x)\} \subseteq F[x]$. Show that the splitting field of S is same as the splitting field of the product $f_1(x)f_2(x)\cdots f_n(x)$.

19. Let K/F be an algebraic extension. Let $a \in K$ with $\deg(\min(F, a)) = n$. Show that $F(a)/F$ is Galois if and only if $\min(F, a)$ has n distinct roots in $F(a)$.

20. Is $\mathbb{F}_2(x)/\mathbb{F}_2(x^2)$ as in Exercise 1, a Galois extension?

21. Show that extensions of degree 2 are always normal. Find an extension K/F of degree 3 which is not normal.

22. Is $\mathbb{C}$ normal over $\mathbb{Q}$? Find a finite normal extension K over $\mathbb{Q}$ that contains a root of $x^4 - 2 \in \mathbb{Q}[x]$. What is $\mathrm{Gal}(K/\mathbb{Q})$?

23. Let $F \subseteq L \subseteq K$ be extensions with K/F normal. Show that K/L is normal and argue that L/F may not be a normal extension.

24. Determine splitting fields of $x^4 - 7$ over (i). $\mathbb{Q}$, (ii). $\mathbb{F}_5$, and (iii). $\mathbb{F}_{11}$.

25. Show that all finite fields are normal extensions over their prime subfields.

26. Let $K := \{x \in \mathbb{C} : x \text{ is algebraic over } \mathbb{Q}\}$. Show that K is a field. Is K algebraically closed?

27. Let $K = F(x_1, x_2, \cdots, x_n)$ be the field of rational functions in n variables over F. Show that there exists a subfield $L \subseteq K$ such that $\mathrm{Gal}(K/L) = S_n$.

28. Let $K = \mathbb{F}_p(a_1, a_2, \cdots, a_n)$ be such that each $a_i^p \in \mathbb{F}_p$. Show that $K/\mathbb{F}_p$ is a normal extension. Determine $\mathrm{Gal}(K/\mathbb{F}_p)$.

29. Convince yourself that there are infinitely many normal extensions K/F for which $\mathrm{Gal}(K/F)$ is trivial.

30. If K/F is a separable extension and L is an intermediate field then show that both K/L and L/F are separable.

31. Let K/F be an extension and $\alpha, \beta \in K$ be separable over F. Show that $\alpha + \beta$ and $\alpha\beta$ are also separable over F.

32. Let K/F be an algebraic extension and $\alpha \in K$ be an element that is not separable over F. Show that $\alpha^{p^r} \in F$ for some integer $r \geq 1$, where $p = \text{char}(F) > 0$.

33. Let F be a field with $\text{char}(F) = p > 0$. Assume that $a \in F$ doesn't have a p^{th} root in F. Show that $x^p - a \in F[x]$ is irreducible over F.

34. Determine if the splitting fields in Exercise 4 above are Galois extensions.

Dr. Dinesh Khurana from Panjab University, Chandigarh delivered two lectures on Algebraic Number Theory and three lectures on Field Theory. In the first lecture on Algebraic Number Theory the participants were given the overview of the subject demonstrating by different examples how the unique factorization property of certain integral domains helps in solving some problems in Number Theory. For instance using the unique factorization property of $\mathbb{Z}[i]$ the characterization of Pythagorean triples and integers that can be written as sum of two squares was achieved. Similarly the unique factorization property of $\mathbb{Z}[\sqrt{-2}]$ was used to solve the Diophantine equation $y^2 + 2 = x^3$. It was also demonstrated how the failure of unique factorization property in $\mathbb{Z}[\omega]$, for several primes p, where ω is a primitive pth root of unity, makes the Fermat's Last Theorem such a hard result.

In the second lecture on Algebraic Number Theory the basic properties of S-integral elements of a ring R, where S is a subring of R, were discussed. Several equivalent conditions for an element of R to be S-integral were discussed which led to the fact that the set of all elements of R that are S-integral forms a subring. Also the transitivity of integral property was discussed. Integral closures and integrally closed domains were discussed. The rings of integers of quadratic number fields were characterized.

The following exercises were discussed in tutorials.

1. Prove that in domains primes are irreducibles.

2. Prove that 2 in $\mathbb{Z}[\sqrt{-d}]$, $d > 2$, is irreducible but not prime.

3. If a, b, c are elements of a UFD R such that $ab = c^n$, $n \in \mathbb{N}$, and a, b are coprime, then prove that a also is nth power of some element of R.

4. Prove that the above result may not hold if R is not a UFD

5. If the prime p is congruent to one modulo four, then prove that the representation of p as a sum of two squares is unique.

6. Let $S \subset R$ and R' be the set of all S-integral elements of R. Prove that R' is integrally closed in R.

7. Prove that the ring of integers of a quadratic number field is a free abelian group of rank two.

In the three lectures on Field Theory the solvability by radicals was discussed. After discussing briefly the history of solvability by radicals, the basic properties of solvable groups and symmetric groups were discussed. It was proved that if a polynomial is solvable by radicals, then its Galois group is solvable. This was used to construct polynomials over the field of rationals that are not solvable by radicals. Finally it was proved that if the Galois group of a polynomial is solvable, then it is solvable by radicals. In the tutorials the following problems were discussed.

1. Prove that S_4 is not generated by $(1\,3)$ and $(1\,2\,3\,4)$.

2. Find all normal subgroups of S_n.

3. Find commutator subgroups of S_n and A_n.

4. Prove that a finite solvable group has a subnormal series whose each factor group is cyclic

5. Construct an example of a polynomial of degree p for every off prime p whose Galois group is S_p.

Dr. Anjana Khurana from Panjab University, Chandigarh delivered three lectures on Field Theory. She covered the following topics.

1. Finite Fields

2. Cyclotomic Extensions

3. Abelian Extensions

4. Cyclic extensions

The characterization, construction and basic properties of finite fields were discussed. Having done basics of Galois theory and fundamental theorem of Galois theory, the participants were shown its applications to study finite extensions of finite fields. Later the extensions $F(w)/F$, where w is an nth root of unity were also discussed. The irreducibility of nth cyclotomic polynomial over rationals and its factorizations over finite fields of characteristic not diving n were done. It was proved that every finite abelian group can be realized as Galois group over the field of rational numbers. Galois extensions with cyclic Galois groups were done in detail.

Following related problems were given and discussed in the tutorials:

Tutorial 1, June 11.

1. Find $G = Gal(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$, the subgroups of it and the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2}, \omega)$.

2. Let $f(x) = x^n - t \in \mathbb{C}(t)[x]$. Find the splitting field K of $f(x)$ and $Gal(K/\mathbb{C}(t))$. Find all intermediate subfields between K and $\mathbb{C}(t)$.

3. Prove the fundamental theorem of algebra using Galois theory.
(*Hint:*

(1) $\mathbb{R}$ has no finite extension of odd degree.
(2) $\mathbb{C}$ has no quadratic extension.)

4. Let F be a finite field. Prove that there is an irreducible polynomial of degree n for every $n \geq 1$ over F.

5. Show that every element of a finite field is a sum of two squares.

6. Show that $f_1(x) = x^4 + x^3 + 1$ and $f_2(x) = x^4 + x + 1$ are irreducible over $\mathbb{F}_2$. Give an explicit isomorphism of fields $\mathbb{F}_2[x]/(f_1(x))$ and $\mathbb{F}_2[x]/(f_2(x))$.

Tutorial 2, June 13.

1. Prove that 5 is a square in $\mathbb{F}_{p^2}$ for every prime p.

2. Prove that every element of $\mathbb{F}_p$ is square in $\mathbb{F}_{p^2}$.

3. If $f(x)$ is an irreducible polynomial of odd degree in $\mathbb{Q}[x]$ then prove that -1 is not a sum of squares in $\mathbb{Q}[x]/(f(x))$.

4. Prove that $\cos(\alpha\pi)$ and $\sin(\alpha\pi)$ are algebraic numbers of every rational α.

5. Prove that $2\cos(\alpha\pi)$ and $2\sin(\alpha\pi)$ are algebraic integers of every rational α.

6. If n is odd prove that $\Phi_{2n}(x) = \Phi_n(-x)$.

7. If F is a finite field of characteristic $\neq 2$ then half the elements of $\mathbb{F}_p^*$ are squares and half are non-squares.

8. Let $F(\sqrt[n]{a})$ be a cyclic extension of F where F contains all the n-th roots of unity. Prove that all intermediate subfields of $F(\sqrt[n]{a})$ are of the form $F(\sqrt[m]{a})$ where $m|n$.

Dr. D. S. Ramana from HRI, Allahabad delivered ten lectures on Algebraic Number Theory.

Lecture 1, June 6. Introduction to number fields, algebraic elements and integers, norms of algebraic numbers, norms of ideals in the ring of integers of a number field and their multiplicative property, discrete subgroups of $\mathbb{R}^n$.

Lecture 2, June 7. Discrete subgroups of $\mathbb{R}^n$, lattices in $\mathbb{R}^n$, Minkowski's theorem on lattice points in measurable subset of $\mathbb{R}^n$.

Tutorial 1, June 7. Discussed the structure theorem of finitely generated modules over PID by dividing the proof into several small steps.

Lecture 3, June 8. Minkowski's theorem on existence of non-zero lattice points, the canonical embedding of a number field into Euclidean space $\mathbb{R}^n$, the image of ring of integers under canonical embedding is a lattice.

Lecture 4, June 9. Applications of Minkowski's theorem: in a number field of degree n, given a non-zero ideal I of ring of integers, there exists an $x \in I$ non-zero such that $|N(x)| \leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} |d|^{1/2} N(I)$ where d is the discriminant of K, and $2r_2$ is the number of complex embeddings of K into $\mathbb{C}$. The proof was application of Minkowski's theorem applied to a convex compact subset of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ defined below for suitable $t > 0$:

$$B_t := \{(y_1, \cdots, y_{r_1}, z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum |y_i| + \sum |z_i| \leq t\}.$$

The computation of volume of this subset was done through a different technique of integration.

Tutorial 2, June 9. Discussed proof of fundamental theorem of finitely generated modules over PID via Smith normal forms, computation of volumes of certain compact subsets of $\mathbb{R}^n$ by method of integration.

Lecture 5, June 11. Dirichlet's unit theorem in number fields, finiteness of principle ideals of a given norm, the units in ring of algebraic integers are precisely the elements of norm 1, the embedding of number field K into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is an $\mathbb{Q}$-algebra homomorphism in which units go to elements of norm 1 in the algebra $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Lecture 6, June 12. Completed the proof of Dirichlet's unit theorem using canonical and logarithmetic embeddings of number fields into Eudlidean spaces. Introduced Noetherian rings and Dedekind domains.

The main aim of above lectures was Dirichlet's unit theorem; it was thoroughly discussed highlighting the essential steps in its proof. These lectures covered most of the part of Chapter IV of the book Algebraic Theory of Numbers by P. Samuel. The essential part of Chapter II of the same book for Dirichlet's theorem was discussed during the lectures according to the need.

Lecture 7, June 13. Characterization of Noetherian domains and their basic properties, a generalization of Dirichlet's theorem: if A is a ring which is finitely generated module over $\mathbb{Z}$ then its group of units is a finitely generated abelian group.

Lecture 8, June 14. Dedekind domains, the integral extensions of Dedekind domains and Dedekind domains; as a consequence, the ring of integers in a number field is a Dedekind domain.

Tutorial, June 14. Integral extensions of Dedekind domains are integrally closed in their field of fractions, discussed the group of units in imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$, $d < 0$ square-free integer.

Lecture 9, June 15. Discussed the existence and uniqueness of factorization of ideals in Dedekind domains.

Lecture 10, June 16. Finiteness of ideal class group in a number field, the group of units in real quadratic extensions of $\mathbb{Q}$.

These lectures were oriented towards the discussion of Dedekinds theorem on unique factorization of ideals in Dedekind domains.These lectures covered Chapter III of the book Algebraic Theory of Numbers by P. Samuel, and remaining part of Chapter IV.

Dr. Rahul Dattatraya Kitture from IISER Mohali assisted in all the twenty four tutorials of one hour each.