Recitation 2: Field Theory Refresher

Scribe: Tomer Manket

1 Field Extensions

Definition 1. A field L is an extension of a field K, denoted by L/K, if $K \subseteq L$ is a subfield.

Example 2. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}(x)/\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$.

Let L/K be a field extension.

Definition 3. The *degree* of L/K is

$$[L : K] := \dim_K L$$

i.e. the dimension of L as a K-vector space.

Example 4. $[\mathbb{C} : \mathbb{R}] = 2$ as $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

Example 5. $[\mathbb{C}(x) : \mathbb{C}] = \infty$ as the set $\{x^k \mid k \in \mathbb{N}\}$ is linearly independent over $\mathbb{C}$.

Definition 6. An element $a \in L$ is *algebraic* over K if there exists a non-zero polynomial $f \in K[x]$ such that $f(a) = 0$. An element which is not algebraic is called *transcendental*. The extension L/K is *algebraic* if every $a \in L$ is algebraic over K.

Claim 7. *Let $K \subseteq L \subseteq M$ be such that M/L and L/K are algebraic. Then M/K is algebraic.*

Definition 8. Let $a \in L$ be algebraic over K. The *minimal polynomial* of a over K, denoted by $\mathrm{irr}(a, K)$, is the unique monic, irreducible polynomial $f \in K[x]$ such that $f(a) = 0$.

Claim 9. *Let $a \in L$ be algebraic over K. Then* $\deg(\mathrm{irr}(a, K)) = [K(a) : K]$.

Example 10. Let $z \in \mathbb{C} \backslash \mathbb{R}$. Then

$$\mathrm{irr}(z, \mathbb{R}) = (x - z)(x - \overline{z}) = x^2 - 2\mathrm{Re}(z)x + |z|^2.$$

Definition 11. A polynomial $f \in K[x]$ is *separable* if all of its roots in $\overline{K}$ are simple, i.e. f is a product of distinct linear factors in $\overline{K}[x]$.

Definition 12. An element $a \in L$ is *separable* over K if it is algebraic over K and $\mathrm{irr}(a, K)$ is separable. The extension L/K is separable if every $a \in L$ is separable over K.

Example 13. $\sqrt{2} \in \mathbb{R}$ is separable over $\mathbb{Q}$, as in $\overline{\mathbb{Q}}[x]$

$$\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}).$$

Example 14. Consider the extension $\mathbb{F}_2(t^2) \subseteq \mathbb{F}_2(t)$. Then the element $t \in \mathbb{F}_2(t)$ is not separable over $\mathbb{F}_2(t^2)$, since in $\overline{\mathbb{F}_2(t^2)}[x]$

$$\operatorname{irr}(t, \mathbb{F}_2(t^2)) = x^2 - t^2 = (x - t)^2.$$

In particular, the extension $\mathbb{F}_2(t)/\mathbb{F}_2(t^2)$ is not separable.

Definition 15. The extension L/K is *normal* if every irreducible polynomial $p \in K[x]$ which has a root in L, splits over L, i.e.

$$f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$$

where $c \in L^\times$ and $\alpha_1, \dots, \alpha_n \in L$.

Example 16. The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, as $p(x) = x^4 - 2$ is irreducible in $\mathbb{Q}[x]$ and has a root $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$, but in $\mathbb{Q}(\sqrt[4]{2})[x]$ we have

$$p(x) = x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x^2 + \sqrt{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2})$$

and $x^2 + \sqrt{2}$ is irreducible in $\mathbb{Q}(\sqrt[4]{2})[x]$ (its roots in $\overline{\mathbb{Q}}[x]$ are $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$).

Definition 17. The extension L/K is called *Galois* if it is normal and separable.

2 Algebraic Independence and Transcendental Bases

Let L/K be a field extension.

Definition 18. A subset $S \subseteq L$ is *algebraically dependent* over K if there exists a subset $\{s_1, \dots, s_n\} \subseteq S$ and a non-zero polynomial $p \in K[x_1, \dots, x_n]$ such that $p(s_1, \dots, s_n) = 0$. Otherwise, S is *algebraically independent* over K.

Remark. Note that $\{s_1, \dots, s_n\} \subseteq L$ is algebraically independent over K if and only if $K[s_1, \dots, s_n] \cong K[x_1, \dots, x_n]$.

Example 19. Let $L := \operatorname{Frac}\left(K[x,y] \big/ \langle y - x^2 + 1 \rangle \right)$. Then $S = \{x, y\} \subseteq L$ is algebraically dependent over K, since for $p(x_1, x_2) = x_2 - x_1^2 + 1$ we have $p(x, y) = 0$.

Definition 20. A *transcendental basis* of L over K is a maximal subset of L that is algebraically independent over K.

Remark. By Zorn's Lemma, every algebraically independent set $S \subseteq L$ can be completed to a maximal algebraically independent set in L. In particular, L/K has a transcendental basis.

Claim 21. *Let $S \subseteq L$ be algebraically independent over K and let $a \in L$. Then*

$$S \cup \{a\} \text{ is algebraically dependent over } K \iff a \text{ is algebraic over } K(S).$$

Proof. ($\Rightarrow$): S is algebraically independent over K while $S \cup \{a\}$ is algebraically dependent over K, so there exist $s_1, \ldots, s_n \in S$ and $0 \neq f \in K[x_1, \ldots, x_{n+1}]$ such that x_{n+1} appears in f and $f(s_1, \ldots, s_n, a) = 0$. Then $f_a := f(s_1, \ldots, s_n, x) \in K(S)[x]$ is non-zero with $f_a(a) = 0$, hence a is algebraic over $K(S)$.

($\Leftarrow$): Left as an exercise. ☐

Corollary 22. *Let $S \subseteq L$ be algebraically independent over K. Then*

$$S \text{ is a transcendental basis of } L/K \iff L/K(S) \text{ is algebraic.}$$

Definition 23. The extension L/K is *purely transcendental* if $L = K(S)$ where S is a transcendental basis of L/K.

Remark. Every field extension L/K is a purely transcendental extension followed by an algebraic extension. Indeed, let S be a transcendental basis of L/K. Then $K(S)/K$ is purely transcendental and $L/K(S)$ is algebraic.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{algebraic}"] \\
K(S) \arrow[d, dash, "\text{purely transcendental}"] \\
K
\end{tikzcd}$$

Theorem 24. *Let A, B be transcendental bases of L over K. Then $|A| = |B|$.*

Proof. We prove the theorem in case L/K has a *finite* transcendental basis $S = \{s_1, \ldots, s_n\}$. Let A be another transcendental basis of L/K. It suffices to show that $|A| \leq n$. ☐

Definition 25. The *transcendence degree* of L/K, denoted by $\operatorname{tr.deg}(L/K)$, is the cardinality of a transcendental basis of L over K.

Example 26. $\operatorname{tr.deg}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \operatorname{tr.deg}(\mathbb{C}/\mathbb{R}) = 0$ as both are algebraic extensions.

Example 27. $\operatorname{tr.deg}(K(x_1, \ldots, x_n)/K) = n$.

Example 28. $\operatorname{tr.deg}(\mathbb{Q}(\pi, e)/\mathbb{Q}) \in \{1, 2\}$. The precise answer is still unknown.

Claim 29. *Let $K \subseteq L \subseteq M$ be field extensions. Then*

$$\operatorname{tr.deg}(M/K) = \operatorname{tr.deg}(M/L) + \operatorname{tr.deg}(L/K).$$