Math 210B Lecture 25 Notes

Daniel Raban

March 11, 2019

1 Solvability by Radicals and Integral Extensions

1.1 Solvability by radicals

Theorem 1.1. *Let $f \in F[x]$ be nonconstant with splitting field K of degree not divisible by* $\operatorname{char}(F)$*. Then K is solvable by radicals if and only if* $\operatorname{Gal}(K/F)$ *is solvable.*

Proof. Let $n = [K : F]$, let $L = K(\zeta_n)$, and let $E = F(\zeta_n)$, where $\langle \zeta_n \rangle = \mu_n$. We claim that K/F is solvable by radicals iff L/E is solvable by radicals. For ($\implies$), we adjoin the same roots of unity. For ($\impliedby$), if L/E is solvable by radicals, then L/F is solvable by radicals. Then K/F is solvable by radicals because $K \subseteq L \subseteq K_s(\zeta_n)$ (where K_s is as in the definition of solvability by radicals).

Now $\operatorname{Gal}(L/E) \cong \operatorname{Gal}(K/K \cap E) \leq \operatorname{Gal}(K/F)$, so if $\operatorname{Gal}(K/F)$ is solvable, then $\operatorname{Gal}(L/E)$ is solvable. Conversely, since $\operatorname{Gal}(L/E)$ is solvable, and since $\operatorname{Gal}(K \cap E/F) \subseteq \operatorname{Gal}(E/F)$ is abelian, $\operatorname{Gal}(L/F)$ solvable $\implies$ $\operatorname{Gal}(K/F)$ is solvable.

So we may assume that $\zeta_n \in F$. Suppose K/F is solvable by radicals. There exists $L \supseteq L$ such that L/F is a radical extension. Exercise: we may choose L such that L/F is Galois. (The idea for this is to show that the normal closure of L/F is still radical.) Tbe $\operatorname{Gal}(L/F)$ is salvable since we have fields $F = L_0 \subseteq L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = L$, such that each L_i/L_{i-1} is abelian, and L_i/F is Galois.

Suppose $\operatorname{Gal}(K/F)$ is solvable. Then there exist intermediate fields K_i/F which are normal and $K_s = K$ such that each $\operatorname{Gal}(K_{i+1}/K_i)$ is finite and abelian (given by adjoining n-th roots of elements in the previous field). So K/F is solvable by radicals. □

Corollary 1.1. *If* $\operatorname{char}(F) \nmid 6$ *and K is the splitting field of an irreducible polynomial of degree ≤ 4, then K/F is solvable by radicals.*

Why 4? This is because A_5 is the smallest nonsolvable group.

Example 1.1. $f = 2x^5 - 10x + 5$ has Galois group S_5. It is irreducible by Eisenstein's criterion. It has 3 real roots.

1.2 Integral extensions

Let B be a commutative ring, and let A be a subring of B. B/A is an extension of commutative rings.

Definition 1.1. We say $\beta \in B$ is **integral** over A if β is the root of a monic polynomial in $A[x]$.

Example 1.2. Any element $a \in A$ is integral over a, as it is the root of $x - a$.

Example 1.3. Let L/K be an extension of fields. If β is algebraic over K, then β is integral over K , as it is the root of its minimal polynomial.

Example 1.4. $\sqrt{2}$ is integral over $\mathbb{Z}$ as the root of $x^2 - 2$.

Example 1.5. $(1 - \sqrt{5})/2$ is integral over $\mathbb{Z}$ as the root of $x^2 - x - 1$.

Example 1.6. $1/2$ is not integral over $\mathbb{Z}$. Let $f = \sum_{i=1}^{n} a_i x^i$ with $a_n = 1$, $a_i \in \mathbb{Z}$. Then $f(1/2) \in (1/2)^n + (1/2^{n-1})\mathbb{Z}$, so $f(1/2) \neq 0$.

Definition 1.2. $\beta \in \overline{\mathbb{Q}} \subseteq \mathbb{C}$ is an **algebraic integer** if it is integral over $\mathbb{Z}$.

Definition 1.3. A **number field** is a finite extension of $\mathbb{Q}$.

Proposition 1.1. *Let $\beta \in B$. The following are equivalent.*

1. *β is integral over A.*
2. *There exists $n \geq 1$ such that $\{1, \beta, \ldots, \beta^{n-1}\}$ generates $A[\beta]$ as an A-module.*
3. *$A[\beta]$ is finitely generated as an A-module.*
4. *There exists an $A[\beta]$-submodule M of B that is finitely generated over A and faithful (i.e. $\mathrm{Ann}_{A[\beta]}(M) = 0$).*

Proof. (1) $\implies$ (2): There exists a monic $f \in A[x]$ of degree n with $f(\beta) = 0$. Then $f(x) = x^n + \sum_{i=1}^{n-1} a - i - 1x^i$, so $\beta^n = -\sum_{i=1}^{n-1} a_{i-1}\beta^i \in A(1, \beta, \ldots, \beta^{n-1})$. By recursion, $\beta^m \in A(1, \beta, \ldots, \beta^{n-1})$ for all $M \geq n$. So $A[\beta]$ is generated by $\{1, \beta, \ldots, \beta^{n-1}\}$ as an A-module.

(2) $\implies$ (3): This is a special case.

(3) $\implies$ (4): Let $M = A[\beta]$. Then $\mathrm{Ann}_{A[\beta]}(A[\beta]) = 0$ since $A[\beta]$ is free over $A[\beta]$.

(4) $\implies$ (1): $M = \sum_{i=1}^{n} A\gamma_i \subseteq B$ for some $\gamma_i \in B$. Without loss of generality, suppose $\beta \neq 0$. Then $\beta\gamma_i = \sum_{j=1}^{n} a_{i,j}\gamma_j$, where $a_{i,j} \in A$. So we can form a linear transformation $T : A^n \to A^n$ by $[T]_{i,j} = a_{i,j}$. Then $f = c_T(x)$. Since $f(\beta) : M \to M$ is 0 and M is faithful, $f(\beta) = 0$. □

Example 1.7. $1/2 \in \mathbb{Q}$ is not integral over $\mathbb{Z}$ since $\mathbb{Z}[1/2]$ is not $\mathbb{Z}$-finitely generated.

Definition 1.4. B/A is an **integral extension** if eery $\beta \in B$ is integral over A.

Example 1.8. $\mathbb{Z}[\sqrt{2}]/\mathbb{Z}$ is an integral extension. It suffices to show that $\alpha = a + b\sqrt{2}$ is always the root of a polynomial. Take the polynomial $x^2 + 2az + (a^2 - 2b^2)$.

Example 1.9. Let B be a finitely generated A-module, and let M be a finitely generated B-module. Then M is a finitely generated A-module.

Next time, we will prove the following.

Proposition 1.2. *Let $B = A[\beta_1, \ldots, \beta_n]$. The following are equivalent.*

1. *B is integral over A.*
2. *Each β_i is integral over A.*
3. *B is finitely generated as an A-module.*