MATH200C, LECTURE 5

GOLSEFIDY

Solvability by radicals (continue)

Proposition 1. *Suppose* $\mu_n := \{\zeta \in F | \, \zeta^n = 1\}$ *has* n *distinct elements,* $\mathrm{Gal}(E/F) \simeq \mathbb{Z}/n\mathbb{Z}$. *Then there is* $a \in F$ *such that* $E = F[\sqrt[n]{a}]$.

Proof. As we have mentioned earlier μ_n is a cyclic group of order n. Suppose $\mu_n = \langle \zeta_n \rangle$. Then $N_{E/F}(\zeta_n) = \zeta_n^n = 1$. Hence by Hilbert's Theorem 90, there is $\beta \in E$ such that $\zeta_n = \frac{\sigma(\beta)}{\beta}$ where σ is a generator of $\mathrm{Gal}(E/F)$; this means $\sigma(\beta) = \zeta_n \beta$. Then $\sigma(\beta^n) = (\zeta_n \beta)^n = \beta^n$; and so β^n is fixed by $\mathrm{Gal}(E/F)$, which means $a := \beta^n \in F$. Notice that a splitting field of $x^n - a$ is $F[\beta]$ as $x^n - a = \prod_{i=0}^{n-1}(x - \zeta_n^i \beta)$ and $\zeta_n \in F$. So $F[\beta]/F$ is a Galois extension. As $\sigma(\beta) = \zeta_n \beta$, we have $\sigma^i(\beta) = \zeta^i \beta$. Hence $o(\sigma|_F[\beta]) = n$, which implies that $[F[\beta] : F] \geq n$. Therefore $E = F[\beta] = F[\sqrt[n]{a}]$; and claim follows. □

Theorem 2. *Suppose* F *is a characteristic zero field,* $f(x)$ *is irreducible in* $F[x]$, *and* E *is a splitting field of* $f(x)$ *over* F. *Suppose* $\mathrm{Gal}(E/F)$ *is solvable. Then* $f(x)$ *is solvable by radicals over* F.

Proof. Suppose $n := |\mathrm{Gal}(E/F)|$. Let L be a splitting field of $f(x)(x^n - 1)$ over F. Then L/F is a Galois extension, E can be viewed as a subfield of L, and $L = F[\text{zeros of } f, \zeta_n] = E[\zeta_n]$ where $x^n - 1 = \prod_{i=0}^{n-1}(x - \zeta_n^i)$. Then

$$1 \to \underbrace{\mathrm{Gal}(L/E)}_{\text{can be embedded into } (\mathbb{Z}/n\mathbb{Z})^\times} \to \mathrm{Gal}(L/F) \to \underbrace{\mathrm{Gal}(E/F)}_{\text{solvable}} \to 1$$

is a S.E.S.; and so $\mathrm{Gal}(L/F)$ is solvable. Hence $\mathrm{Gal}(L/F[\zeta_n])$ is solvable. Therefore there is a chain of subgroups $\{N_i\}_i$ such that

$$1 = N_k \trianglelefteq N_{k-1} \trianglelefteq \cdots \trianglelefteq N_1 = \mathrm{Gal}(L/F[\zeta_n]),$$

and $N_{i-1}/N_i \simeq \mathbb{Z}/m_i\mathbb{Z}$. Notice that

$$[L : F[\zeta_n]] = \frac{[L : F]}{[F[\zeta_n] : F]} = \frac{[E[\zeta_n] : E]}{[F[\zeta_n] : F]}[E : F]$$

and $\mathrm{Gal}(E[\zeta_n]/E)$ can be embedded into $\mathrm{Gal}(F[\zeta_n]/F)$. Hence

$$m_i|[L : F[\zeta_n]], \text{ and } [L : F[\zeta_n]]|[E : F] = n.$$

Let $L_i := \mathrm{Fix}(N_i)$. Then, for any i, we have that L_i/L_{i-1} is a Galois extension and $\mathrm{Gal}(L_i/L_{i-1}) \simeq \mathbb{Z}/m_i\mathbb{Z}$, $\zeta_n \in L_{i-1}$, and $m_i|n$. Thus by the previous proposition, there is $a_{i-1} \in L_{i-1}$ such that $L_i = L_{i-1}[\sqrt[m_i]{a_{i-1}}]$; and claim follows. □

Commutative algebra

As it has been pointed out a lot of algebra has been developed to understand zeros of polynomials. We have seen how Galois theory was developed to understand zeros of single variable polynomials. Next we will try to understand either zeros of single variable polynomials in $\mathbb{Z}$ (instead of $\mathbb{Q}$) (going towards algebraic number theory) or zeros of multivariable polynomials in $\overline{\mathbb{Q}}$ (going towards algebraic geometry).

Long ago we have seen that $\mathrm{Nil}(A) = \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}$, $\mathrm{Nil}(A)$ is called the nilradical of A. Let $J(A) := \bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m}$; $J(A)$ is called the Jacobson radical of A. Jacobson has defined this concept for non-commutative rings; he defined left and right Jacobson radicals as the intersection of maximal left and right ideals respectively; and then showed they are equal. Therefore it is an ideal. It is an important concept as simple A-modules are the same as simple $A/J(A)$-modules. In this course we work only with commutative rings. Here is a basic property of $J(A)$.

Lemma 3. $x \in J(A) \Leftrightarrow \forall y \in A, 1 - xy \in A^\times$.

Proof. ($\Rightarrow$) Suppose to the contrary that there is $y \in A$ such that $1 - xy \notin A^\times$; then the ideal generated by $1-xy$ is a proper ideal of A. Hence there is a maximal ideal $\mathfrak{m} \in \mathrm{Max}(A)$ such that $1 - xy \in \mathfrak{m}$. Since $x \in J(A)$, $x \in \mathfrak{m}$. Therefore $1 \in \mathfrak{m}$, which is a contradiction.

($\Leftarrow$) Suppose for some $\mathfrak{m} \in \mathrm{Max}(A)$ we have that $x \notin \mathfrak{m}$. Then $x + \mathfrak{m}$ is a non-zero element of the field $A/\mathfrak{m}$. Thus there is $y \in A$ such that $xy \equiv 1 \pmod{\mathfrak{m}}$, which means $1 - xy \in \mathfrak{m}$. Thus $1 - xy \notin A^\times$ which is a contradiction. □

Proposition 4. *(1)* $\mathrm{Nil}(A[x]) = (\mathrm{Nil}(A))[x]$.
(2) $(A[x])^\times = \{\sum_{i=0}^{\infty} a_i x^i \in A[x] |\ a_0 \in A^\times, a_i \in \mathrm{Nil}(A) \text{ if } i \geq 1\}$.
(3) $J(A) = (\mathrm{Nil}(A))[x]$.

Proof. (1) Since $\mathrm{Nil}(A[x])$ is an ideal of $A[x]$ and $\mathrm{Nil}(A)$ is a subset of $\mathrm{Nil}(A[x])$, we have that $\mathrm{Nil}(A[x]) \supseteq (\mathrm{Nil}(A))[x]$.

For any $\mathfrak{p} \in \mathrm{Spec}(A)$, we have that $A[x]/\mathfrak{p}[x] \simeq (A/\mathfrak{p})[x]$ is an integral domain. Hence $\mathfrak{p}[x]$ is in $\mathrm{Spec}(A[x])$ if $\mathfrak{p} \in \mathrm{Spec}(A)$. Therefore

$$\mathrm{Nil}(A[x]) \subseteq \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}[x] = (\mathrm{Nil}(A))[x];$$

and claim follows.

(2) In any ring B, if $u \in B^\times$ and $n \in \mathrm{Nil}(B)$, then $u + n \in B^\times$: $u + n = u(1 + u^{-1}n)$ and $(1 + y)(1 - y + y^2 - \cdots + (-1)^k y^k) = 1$ if $y^{k+1} = 0$. So the RHS consists of units. Suppose $f(x) = \sum_{i=0}^{\infty} a_i x^i \in (A[x])^\times$; that means for some $g(x) = \sum_{i=0}^{\infty} b_i x^i \in A[x]$, $f(x)g(x) = 1$. Thus $1 = f(0)g(0) = a_0 b_0$; and so $a_0 \in A^\times$. For any $\mathfrak{p} \in \mathrm{Spec}(A)$, we have $f(x)g(x) \equiv 1 \pmod{\mathfrak{p}}$. Since $A/\mathfrak{p}$ is an integral domain, $(A/\mathfrak{p})[x]^\times = (A/\mathfrak{p})^\times$. This implies that $a_i \in \mathfrak{p}$ for $i \geq 1$ and $\mathfrak{p} \in \mathrm{Spec}(A)$. Hence $a_i \in \bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} = \mathrm{Nil}(A)$ for $i \geq 1$; and claim follows.

(3) Clearly $J(A) \supseteq \mathrm{Nil}(A[x]) = (\mathrm{Nil}(A))[x]$. Suppose $f(x) \in J(A)$; then $1 - xf(x) \in A[x]^\times$. Thus all the coefficients of $f(x)$ are in $\mathrm{Nil}(A)$, which means $f(x) \in (\mathrm{Nil}(A))[x]$. □

Let's recall that we say an ideal $\mathfrak{a}$ divides $\mathfrak{b}$ and write $\mathfrak{a}|\mathfrak{b}$ if $\mathfrak{b} \subseteq \mathfrak{a}$. We denote the set of prime divisors of an ideal $\mathfrak{a}$ by $V(\mathfrak{a})$.

Proposition 5 (Basics of divisibility for ideals)**.** *(1)* $\mathfrak{a}|\mathfrak{b} \Rightarrow V(\mathfrak{a}) \subseteq V(\mathfrak{b})$.

(2) $\gcd(\{\mathfrak{a}_i\}_{i\in I}) = \sum_{i\in I} \mathfrak{a}_i$ *and* $V(\sum_{i\in I} \mathfrak{a}_i) = \bigcap_{i\in I} V(\mathfrak{a}_i)$.

(3) $\mathrm{lcm}(\{\mathfrak{a}_i\}_{i\in I}) = \bigcap_{i\in I} \mathfrak{a}_i$ *and* $V(\bigcap_{i=1}^n \mathfrak{a}_i) = \bigcup_{i=1}^n V(\mathfrak{a}_i)$*; for an infinite family of ideals equality does not necessarily hold.*

(4) $V(A) = \varnothing$ *and* $V(0) = \mathrm{Spec}(A)$.

Proof. (1) One can see that $\mathfrak{a}|\mathfrak{b}$ and $\mathfrak{b}|\mathfrak{c}$ imply that $\mathfrak{a}|\mathfrak{c}$. Hence if $\mathfrak{a}|\mathfrak{b}$, then any prime divisor of $\mathfrak{a}$ is a prime divisor of $\mathfrak{b}$.

(2) $\mathfrak{b}|\mathfrak{a}_i$ for any i implies that $\mathfrak{a}_i \subseteq \mathfrak{b}$ for any i; and so $\sum_{i\in I} \mathfrak{a}_i \subseteq \mathfrak{b}$ which implies that $\mathfrak{b}|\sum_{i\in I} \mathfrak{a}_i$. Clearly $\mathfrak{a}_j \subseteq \sum_{i\in I} \mathfrak{a}_i$ which means $\sum_{i\in I} \mathfrak{a}_i|\mathfrak{a}_j$ for any j. As $\gcd(\{\mathfrak{a}_i\}_{i\in I}|\mathfrak{a}_j$, $V(\sum_{i\in I} \mathfrak{a}_i) \subseteq V(\mathfrak{a}_j)$ for any j. If $\mathfrak{p} \in \bigcap_i V(\mathfrak{a}_i)$, then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for any i; this implies that $\sum_{i\in I} \mathfrak{a}_i \subseteq \mathfrak{p}$.

(3) $\forall i \in I, \mathfrak{a}_i|\mathfrak{b} \Leftrightarrow \forall i \in I, \mathfrak{b} \subseteq \mathfrak{a}_i \Leftrightarrow \mathfrak{b} \subseteq \bigcap_i \mathfrak{a}_i \Leftrightarrow (\bigcap_i \mathfrak{a}_i)|\mathfrak{b}$. Since $\mathfrak{a}_i|\bigcap_j \mathfrak{a}_j$, $V(\mathfrak{a}_i) \subseteq V(\bigcap_j \mathfrak{a}_j)$; and so $\bigcup_{i\in I} V(\mathfrak{a}_i) \subseteq V(\bigcap_{i\in I} \mathfrak{a}_i)$. Suppose to the contrary that

$\mathfrak{p} \in V(\bigcap_{i=1}^n \mathfrak{a}_i) \setminus \bigcap_{i=1}^n V(\mathfrak{a}_i)$; then $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$ and for any i there is $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$. Therefore $\prod_{i=1}^n a_i \notin \mathfrak{p}$ and $\prod_{i=1}^n a_i \in \bigcap_{i=1}^n \mathfrak{a}_i$, which contradicts $\bigcap_{i=1}^n \mathfrak{a}_i \subseteq \mathfrak{p}$.

Let $\mathscr{P}$ be the set of prime numbers in $\mathbb{Z}$. Then $\bigcap_{p\in\mathscr{P}} p\mathbb{Z} = 0$; and so 0 is in $V(\bigcap_{p\in\mathscr{P}} p\mathbb{Z})$; but 0 is not in $\bigcup_{p\in\mathscr{P}} V(p\mathbb{Z})$.

(4) is clear. □

Definition 6 (Zariski topology)**.** *Let* $\{V(\mathfrak{a})\}_{\mathfrak{a}\trianglelefteq A}$ *be the set of closed subsets of* $\mathrm{Spec}(A)$*. The above proposition shows that this collection of closed sets give us a well-defined topology on* $\mathrm{Spec}(A)$*. This is called the Zariski topology of* $\mathrm{Spec}(A)$*.*