172 — 6

RJ Acuña

(862079740)

1. Recall that $\mathbb{C}(t) := \{f(t)/g(t) \mid f, g \in \mathbb{C}[t]\ g \neq 0\}$ is the field of rational functions in a variable t with coefficients in $\mathbb{C}$. Show that $\mathbb{C}(t)$ is not algebraically closed.

   pf.

   Consider $X^2 + t \in \mathbb{C}(t)[X]$, Suppose for a contradiction that $f/g \in \mathbb{C}(t)$ solves

$$X^2 + t = 0 \tag{1}$$

   It follows that,

$$\left(\frac{f}{g}\right)^2 + t = 0 \iff \frac{f^2}{g^2} + t = 0 \iff f^2 + tg^2 = 0 \iff f^2 = -tg^2 \iff -t \mid f^2$$

$$f^2 = f \cdot f \text{ and } -t \mid f^2 \implies -t \mid f \implies \exists t \in \mathbb{C}[t] : f = -th$$

$$\implies (-th)^2 = -tg^2 \iff (-th)^2 + tg^2 = 0 \iff t^2h^2 + tg^2 = 0 \iff t(th^2 + g^2) = 0$$

$$\implies g^2 + th^2 = 0 \implies -t \mid g \implies \exists k \in \mathbb{C}[t] : g = -tk$$

   Then $g(0) = -0k$, so $g \neq 0$ is false. Therefore, $f/g \notin \mathbb{C}(t)$ $\rightarrow\leftarrow$

   So, $\mathbb{C}(t)$ is not algebraically closed ■

2. Suppose that $F \subset E$ is a finite field extension (so E is finite dimensional as a vector space over F). Show that if $F \subset R \subset E$ and R is a ring, then R is a field.

   pf.

   Let F be a field, and $F \subset E$ be a finite field extension. Then E is a finite dimensional vector space over F of dimension n. Let $\{\mathrm{e}_i\}_{i=1}^n$ be a basis for E.

   $R \subset E \implies \forall \mathrm{r} \in R, \exists! t_i \in F : \mathrm{r} = \sum_{i=1}^n t_i \mathrm{e}_i$,

   If $R = E$, we're done,

   Notice, $F \subset R \implies 0 \in R$, and since R is a ring it is closed under addition.

   If $R \neq E$ then, $\exists \mathrm{x} \in E : \mathrm{x} \notin R$, Let $\langle \mathrm{x} \rangle$ be the span of x.

   $\forall s \in F, s\mathrm{x} \in \langle \mathrm{x} \rangle$. Suppose $\exists s \in F : s\mathrm{x} \in R$, then

$$F \subset R \text{ and } R \text{ is a ring} \implies \frac{1}{s} \in R \text{ and } \frac{1}{s} s\mathrm{x} = \mathrm{x} \in R \text{ respectively.}$$

   That contradicts that $\mathrm{x} \notin E$. So $\langle \mathrm{x} \rangle \cap R = \{0\}$

   Since $\{\mathrm{x}\}$ is a basis for $\langle \mathrm{x} \rangle$, and since $\dim_F E = n$ we can extend it to a basis$\{\mathrm{x}\} \cup \{\mathrm{u}_i\}_{i=1}^{n-1}$ for E.

   We've shown that $R \subset \langle \mathrm{u}_1, \cdots, \mathrm{u}_{n-1} \rangle$. Now, if $R = \langle \mathrm{u}_1, \cdots, \mathrm{u}_{n-1} \rangle$, then R is a field, as it is a vector subspace of a finite field extension. Otherwise, we can find a $\mathrm{y} \in \langle \mathrm{u}_1, \cdots, \mathrm{u}_{n-1} \rangle$, such that $\{\mathrm{y}\} \cup \{\mathrm{w}_i\}_{i=1}^{n-2}$ is a basis of $\langle \mathrm{u}_1, \cdots, \mathrm{u}_{n-1} \rangle$, and $R \subset \langle \mathrm{u}_1, \cdots, \mathrm{u}_{n-1} \rangle$. This process is finite, since the dimension is n.

   After m steps there is a minimal basis $B = \{\mathrm{v}_i\}_{i=1}^m$, where m satisfies $1 \leq m < n - 1$, such that $R \subset \langle B \rangle$. And, it also satisfies that if we remove any element v_k of the basis B, then $\langle B \backslash \{\mathrm{v}_k\} \rangle \subset R$.

   Let $r \in R$ such that $r \notin \langle B \backslash \{\mathrm{v}_k\} \rangle$, then $F \subset R \implies \exists! t \in F : r = t\mathrm{v}_k$, since $R \subset \langle B \rangle$. So, if there exists such r, it follows that $R = \langle B \rangle$. If, there isn't such an r, then $R = \langle B \backslash \{\mathrm{v}_k\} \rangle$, contradicting the minimality of B. Therefore R is a finite dimensional vector space over F. So, R is a field ■

3. Let R be the smallest subring of $\mathbb{R}$ containing $\mathbb{Q}$ and π, so that $\mathbb{Q} \subset R \subset \mathbb{R}$. Show that R is not a field by showing π^{-1} is not in R.

   pf. Since π, is a transcendental number. It follows that $\forall f(x) \in \mathbb{Q}[x], f(\pi) \neq 0$. Suppose $\pi^{-1} \in \mathbb{Q}[\pi]$, then for some $f(x) = \sum_{k=1}^{n} a_k x^k \in \mathbb{Q}[x]$,

$$\pi^{-1} = \sum_{k=0}^{n} a_k \pi^k \iff 1 = \sum_{k=0}^{n} a_k \pi^{k+1} \iff 0 = -1 + \sum_{k=0}^{n} a_k \pi^{k+1} = h(\pi)$$

$$\implies \exists h(x) \in \mathbb{Q}[x] : h(\pi) = 0 \rightarrow\leftarrow$$

   $\pi^{-1} \notin R = \mathbb{Q}[\pi] \implies R$ is not a field ■

4. Let F be a finite field with p^n elements (which we showed in class is automatically a field extension of $\mathbb{Z}/p\mathbb{Z}$). Suppose that $\alpha \in F$ generates the group $F^\times$ of units in F. Show that $deg(\alpha; \mathbb{Z}/p) = n$.

   pf.

   By 33.11 for every finite field $\mathbb{Z}/p\mathbb{Z}$, and for every $n \in \mathbb{N}$ there exists an irreducible polynomial $f(x)$ of degree n in $(\mathbb{Z}/p\mathbb{Z})[x]$. Then, since $f(x)$ is irreducible, $\langle f(x) \rangle$ is maximal, therefore $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ is a field. Furthermore, it has p^n elements, sine it is an n-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$, which has p elements. By 33.12 $(\mathbb{Z}/p\mathbb{Z})[x]/\langle f(x) \rangle$ is isomorphic to F. So, deg$(\alpha; \mathbb{Z}/p\mathbb{Z}) =$ deg$f = n$ ■