Intro

OH this week Tu 3PM in MS 3919
Th 12PM

poll for later weeks

HW schedule TBD

The central object in this course is the <u>field extension</u>

Notation. We write K/F to say F is a subfield of the field K.

e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{Q}[i]/\mathbb{Q}$.

We want to begin with a field F and extend it to solve more equations. Our primary method is to form $F[t]/(f)$ for $f \in F[t]$ irreducible. This is a field extension of F via the inclusion

$$\begin{aligned} F &\longrightarrow F[t]/(f) \\ a &\longmapsto a+(f) \end{aligned}$$

Prop. Let $n = \deg(f)$. Then $F[t]/(f)$ is an n-dimensional vector space $/F$ via the previous inclusion.

We write $[F[t]/(f) : F] = \deg(f)$.

Pf. We claim that $\{\bar{1}, \bar{t}, \ldots, \bar{t}^{n-1}\}$ is an F-basis for $F[t]/(f)$.

<u>Lin. indep.</u> Suppose $\sum_{i=0}^{n-1} a_i \bar{t}^i = 0$ in $F[t]/(f)$.

Then $\overline{\sum_{i=0}^{n-1} a_i t^i} = 0$ so $f \mid \sum_{i=0}^{n-1} a_i t^i$ in $F[t]$.

The RHS has degree $\leq n-1 < n = \deg(f)$, so as F is a field (hence a domain), $\sum a_i t^i = 0$. So all $a_i = 0$.

<u>Span</u>. Let $\bar{g} \in F[t]/(f)$. By the division algorithm, $\exists!\, q, r \in F[t]$ so that $g = fq + r$ and $\deg(r) < \deg(f)$. Hence, $\bar{g} = \bar{r}$ and as $\deg(r) < n$, $\bar{r} \in \operatorname{span}\{\bar{1}, \bar{t}, \ldots, \bar{t}^{n-1}\}$.

e.g. $\mathbb{Q}(i) \cong \mathbb{Q}[t]/(t^2+1)$

$i \longleftarrow\!\shortmid \bar{t}$

$\mathbb{C} \cong \mathbb{R}[t]/(t^2+1)$

$i \longleftarrow\!\shortmid \bar{t}$

Prop. In $F[t]/(f)$, f has a root.

pf. $f(\bar{t}) = \overline{f(t)} = 0$ in $F[t]/(f)$.

we call this "adjoining a root of f to F"!

Thm. (Kronecker). Let F be a field and $f \in F[t]$. There exists a field extension K/F so that f splits in K, i.e., it factors into linear terms. Furthermore, $[K:F] \leq \deg(f)!$

pf. We induct on $n = \deg(f)$.

For $n = 0, 1$ we take $K = F$.

Suppose that $n \geq 2$ and that the result holds for all polynomials of degree less than n.

Let $g | f$ be irreducible, let $K' = F[t]/(g)$. Then g has a root in K', so f has a root in K'. Also, $[K':F] = \deg(g) \leq n$.

Hence, in $K'[t]$, we may factor $f = (t-a)f'$, where now $f' \in K'[t]$ has degree $n-1$. Hence, by induction, there is a field extension K/K' of degree $\leq (n-1)!$ so that f' splits. Hence, f splits in K, so it suffices to compute $[K:F]$.

We claim $[K:F] = [K:K'][K':F]$. Indeed, we prove this in general. (Also, compare this to Lagrange's theorem)

Lemma. Let $K/K'/F$ be field extensions.

Let $\mathcal{B} = \{\beta_i\}_{i \in I}$ be an F-basis for K

Let $\mathcal{C} = \{\gamma_j\}_{j \in J}$ be a K'-basis for K

Then $\mathcal{B}\mathcal{C} = \{\beta_i \gamma_j\}_{I \times J}$ is an F-basis for K

Furthermore, the map
$$\begin{aligned} \mathcal{B} \times \mathcal{C} &\longrightarrow \mathcal{B}\mathcal{C} \\ (\beta_i, \gamma_j) &\longmapsto \beta_i \gamma_j \end{aligned}$$

is a bijection

Pf. <u>Bijectivity</u>. $\mathcal{B} \times \mathcal{C} \longrightarrow \mathcal{B}\mathcal{C}$ is surely onto.

suppose $\beta_i \gamma_j = \beta_{i'} \gamma_{j'}$. As the γ's are a K'-basis for K and the β's are a in F, $\beta_i = \beta_{i'}$ and $\gamma_j = \gamma_{j'}$.

<u>Lin inden.</u> Let $\sum_{i,j} a_{ij} \beta_i \gamma_j = 0$ for $a_{ij} \in F$.

we rewrite this as $\sum_j \left(\sum_i a_{ij} \beta_i \right) \gamma_j$.

The γ's are K'-lin indep and $\sum_i a_{ij} \beta_i \in K'$ for all j, so for all j, $\sum_i a_{ij} \beta_i = 0$. Thus, as the β are F-lin indep and the $a_{ij} \in F$, all $a_{ij} \neq 0$.

Spgy Let $x \in K$, Then $x = \sum b_j \gamma_j$ for some $b_j \in K'$.

Each $b_j = \sum_i a_{ij} \beta_i$. Thus, $x = \sum a_{ij} \beta_i \gamma_j$. □

Thus, $[K:F] = [K':K'][K':F]$

$\leq (n-1)!\, n$

$= n!$ □

e.g. $F = \mathbb{Q}$, $f = t^3 - 2$.

Let $K_1 = \mathbb{Q}[t]/(f)$. We write suggestively $\sqrt[3]{2} := \bar{t}$.

This is only one root of f, all of which are cube roots of 2,

and it is not the same as the real number.

In K_1, f factors as $(t - \sqrt[3]{2})\underbrace{(t^2 + \sqrt[3]{2}\, t + \sqrt[3]{2}^2)}_{f'}$

$[K_1 : \mathbb{Q}] = 3$.

Let $K_2 = K_1[t]/(f')$, Then $[K_2 : K_1] = 2$ and f splits in K_2.

If $\alpha \in K_2$ is a root of f', then $\left(\frac{\alpha}{\sqrt[3]{2}}\right)^3 = 1$ and $\frac{\alpha}{\sqrt[3]{2}} \neq 1$.

Thus, $\frac{\alpha}{\sqrt[3]{2}}$ is a primitive 3rd root of unity. We could have also gotten K_2 as $K_1[t]/(t^3+t+1)$, which adjoins a primitive 3rd root of unity to K_1.

Defining maps We saw above that we often construct fields by iterating the construction $F \rightsquigarrow \frac{F[t]}{(f)}$.

We now want to understand how to define maps out of $F[t]/(f)$, given a map out of F. This provides the essential recursion to define maps out of fields.

Thm. Let R be a ring and let $\varphi : F \longrightarrow R$. Let $f \in F[t] - F$. Then there is a bijection

$$\begin{array}{c} \{\text{maps } F[t]/(f) \xrightarrow{\Phi} R \text{ s.t. } \Phi|_F = \varphi\} \\ \big\downarrow\wr \\ \{\alpha \in R \mid f(\alpha) = 0\} \end{array}$$

$\Phi \longmapsto \Phi(\bar{t})$

Pf. Let $\alpha \in R$ s.t. $f(\alpha) = 0$. Then let $F[t] \longrightarrow R$ via $\sum a_i t^i \longmapsto \sum a_i \alpha^i$.

Then as $f(\alpha) = 0$, (f) is in the kernel and the map factors as $F[t]/(f) \longrightarrow R$, $\bar{t} \longmapsto \alpha$. This is inverse to above. $\square$