Lecture 11: Multiplication in fields as linear transformations

Last time: $F \subseteq K_1, K_2 \subseteq L$

Compositum: K_1K_2 = smallest subfield of L containing K_1 and K_2.

Thm: $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$

[When proving this thm used an important idea I will expand on today...]

Setting: $F \subseteq K$ fields. K is an F-vector space.

Fix $r \in K$. Then $T: K \to K$, $s \mapsto rs$ is an F-linear transformation: $T(\overset{\text{in } F}{f} \cdot s) = rfs = frs = f \cdot T(s)$ and $T(s_1 + s_2) = r(s_1 + s_2) = rs_1 + rs_2 = T(s_1) + T(s_2)$.

Ex: $F = \mathbb{R}$, $K = \mathbb{C}$, $r = 1 + 2i$. The matrix of $T_r : \mathbb{C} \to \mathbb{C}$ with respect to the $\mathbb{R}$-basis $\{1, i\}$ is $\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$ since

$$T_r(1) = 1 + 2i = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$
$$T_r(i) = -2 + i = \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

More generally, the matrix for T_r with $r = a+bi$ is $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

[ring of 2×2 matrices with $\mathbb{R}$ entries]

<u>Claim:</u>
$$\begin{aligned} \mathbb{C} &\longrightarrow M_2(\mathbb{R}) \\ r &\longmapsto [T_r]_{\mathcal{B}} \end{aligned}$$
is a ring homomorphism, with $\mathcal{B} = \{1, i\}$.

<u>Pf:</u>
$$\begin{aligned} \{S : \mathbb{C} \to \mathbb{C} \mid \mathbb{R}\text{-linear}\} &\xrightarrow{\cong} M_2(\mathbb{R}) \\ S &\longmapsto [S]_{\mathcal{B}} \end{aligned}$$

takes composition of linear trans to matrix mult.

So for $r, s \in \mathbb{C}$ we have $(T_r \circ T_s)(z) = rsz = T_{rs}(z)$ gives $[T_r]_{\mathcal{B}}[T_s]_{\mathcal{B}} = [T_{rs}]_{\mathcal{B}}$. Addition is similar, since $T_r(z) + T_s(z) = rz + sz = (r+s)z = T_{r+s}(z)$. ▨

<u>Cor:</u> $\mathbb{C}$ is isomorphic to the subring $\underbrace{\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R}\right\}}_{\text{Field}}$ of $M_2(\mathbb{R})$. In particular

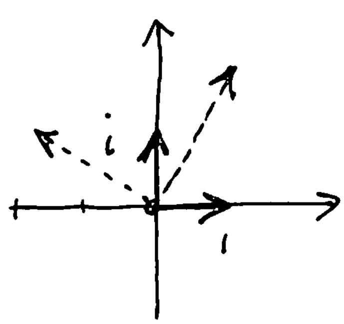
$$\underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{\text{cor to } i}{}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thm: Suppose $[K:F] = n < \infty$. An F-basis $\mathcal{B}$ of K gives a 1-1 ring hom $K \xrightarrow{\psi} M_n(F)$ by $r \longmapsto [T_r]_{\mathcal{B}}$. [Point out usefullness.]

Pf: If $r \in \ker(\psi)$, have $T_r(s) = 0$ for all $s \in K$. In particular $0 = T_r(1) = r$. So $\ker\psi = \{0\}$. $\square$

Any invariant of linear trans gives an invariant of $r \in K$. While $[T_r]_{\mathcal{B}}$ depends on $\mathcal{B}$, its det, trace, and char poly do not.

Ex: $F = \mathbb{R}$, $K = \mathbb{C}$, $r = 1 + 2i$, $[T_r]_{\mathcal{B}} = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$ w/ $\mathcal{B} = \{1, i\}$.

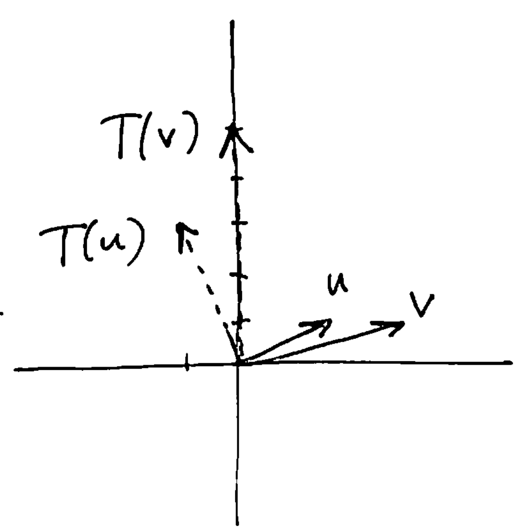


[Note T_r rotates and dilates]

For $\mathcal{B}' = \{\underset{u}{1+i}, \underset{v}{2+i}\}$ get $\begin{pmatrix} 7 & 10 \\ -4 & -5 \end{pmatrix}$

since $T_r(u) = -1 + 3i = 7u - 4v$

$T_r(v) = \quad 5i = 10u - 5v$



Then

$\det T_r = 1 + 2 \cdot 2 = -35 + 40 = 5$

For $z = a+bi$, have

$$\det T_z = \det\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2+b^2 = |z|^2$$

$$\operatorname{tr} T_z = \operatorname{tr}\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = 2a = 2\operatorname{Re}(z)$$

For a general K/F, $\det T_r$ is the <u>norm</u> $N_{K/F}(r)$.

<u>Q</u>: Find the min. poly of $r = 1+2i$ in $\mathbb{R}[x]$.

Set $M = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$, which has char. poly

$$\det(xI - M) = \det\begin{pmatrix} x-1 & 2 \\ -2 & x-1 \end{pmatrix} = (x^2-2x+1)+4$$
$$= x^2-2x+5.$$

Any matrix satisfies its char poly:

$$M^2 - 2M + 5\cdot I = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

As we have a 1-1 ring hom $\mathbb{C} \to M_2(\mathbb{R})$ sending $r \mapsto M$, must have $r^2 - 2r + 5 = 0$.

As $x^2 - 2x + 5$ has no real roots, it is irred and hence $= m_{r,\mathbb{R}}(x)$.

Any M in $M_2(\mathbb{R})$ has char poly $x^2 - (\operatorname{tr} M)x + \det M$

So $z \in \mathbb{C} \setminus \mathbb{R}$ has $m_{z,\mathbb{R}}(x) = x^2 - (2\operatorname{Re} z)x + |z|^2$

Ex: D square-free integer $K = \mathbb{Q}(\sqrt{D})$
$F = \mathbb{Q}$

Then with $\mathcal{B} = \{1, \sqrt{D}\}$ get $[T_{a+b\sqrt{D}}]_{\mathcal{B}} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix}$

and $N_{K/F}(a+b\sqrt{D}) = a^2 - b^2 D$

Cor: $M_2(\mathbb{Q})$ contains subrings isomorphic to infinitely many distinct fields.

A number field is a finite extension $K/\mathbb{Q}$.

An algebraic integer in K is an α where $\exists$ a monic $p(x) \in \mathbb{Z}[x]$ with $p(\alpha) = 0$.

The alg. ints in $\mathbb{Q}(i)$ are $\mathbb{Z}[i]$

The alg ints in $\mathbb{Q}(\sqrt{-3})$ are $\mathbb{Z}[\alpha]$ with $\alpha = \frac{1+\sqrt{-3}}{2}$.

Fact: The set $\mathcal{O}_K$ of all alg. ints in K is a subring. If $[K:\mathbb{Q}] = n$, then $(\mathcal{O}_K, +) \cong (\mathbb{Z}^n, +)$ and any basis for $\mathcal{O}_K$ is one for K.

In such a basis, $[T_\alpha]_{\mathcal{B}} \in M_n(\mathbb{Z})$ for any alg. int. α. In part., $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and α is a unit in $\mathcal{O}_K \iff N_{K/\mathbb{Q}}(\alpha) = 1$.