Lecture 11: Multiplication in rings as linear transformations ①

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

[In proving this theorem, we used an important idea which I'll expand on today...]

Suppose $F \subseteq R$ where R is an integral domain and F is a subring which is also a field.

[For us, R will usually also be field, but here's another ex:]

Ex: F a field, $R = F[[t]] = \left\{ \sum_{n=0}^{\infty} a_n t \mid a_n \in F \right\}$ is an int domain (look at lowest deg. terms), but e.g. t has no mult. inverse.

Note: R is a vector space over F since

$$f(r_1+r_2) = fr_1 + fr_2$$
$$(f_1+f_2)r = f_1r + fr_2$$
$$f_1(f_2r) = (f_1f_2)r$$
$$1_F r = r$$

Uses that $1_F = 1_R$ since R is an integral domain.

Contrast: $R = \mathbb{R} \times \mathbb{R}$

$F = \mathbb{R} \times \{0\}$

$1_F \cdot (0,2) = (0,0)$.

Fix $r \in R$. Then $\begin{aligned} T: R &\to R \\ s &\mapsto rs \end{aligned}$ is an F-linear transformation as $T(fs) = rfs = f(rs) = f \cdot T(s)$ and $T(s_1 + s_2) = r(s_1 + s_2) = rs_1 + rs_2$.

<u>Ex</u>: $F = \mathbb{R}$, $R = \mathbb{C}$, $r = 1 + 2i$, $T_r : \mathbb{C} \to \mathbb{C}$

What is the matrix of T_r with respect to the $\mathbb{R}$-basis $\{1, i\}$?

$$\left.\begin{aligned} T_r(1) &= 1 + 2i = (1, 2) \\ T_r(i) &= i - 2 = (-2, 1) \end{aligned}\right\} \Rightarrow \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$$

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

Suppose $s \in \mathbb{C}$. Then $T_r(T_s(z)) = rsz = T_{rs}(z)$ and $T_r(z) + T_s(z) = T_{r+s}(z)$. This means that

$$\begin{aligned} \mathbb{C} &\longrightarrow M_2(\mathbb{R}) \leftarrow \text{ring of } 2\times 2 \text{ matrices with } \mathbb{R} \text{ entries.} \\ r &\longmapsto \text{Matrix of } T_r \end{aligned}$$

is a <u>ring homomorphism</u>!

That is, $\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$ which is isomorphic to $\mathbb{C}$. In particular

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

cor. to i.

Generalizing, get if $\dim_F R = n < \infty$, then picking a basis $r_1, \ldots, r_n$ gives a ring homom.

$$R \longrightarrow M_n(F)$$
$$r \longmapsto \text{matrix of } T_r \text{ with respect to}$$

which is 1-1 since if $T_r(s) = 0$ for $s \neq 0$ then $r = 0$ as R is an int. domain. So again R is a subring of $M_n(F)$. [Point out usefullness.]

<u>Thm</u>: R int domain containing a field F. If $\dim_F R < \infty$, then R is a field.

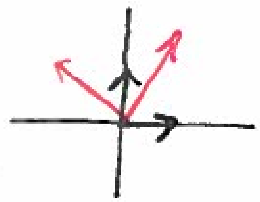
<u>Pf</u>: Let $r \neq 0$ in R and consider $T_r : R \to R$, $s \to rs$. As noted above, $\ker T_r = \{0\}$ and so as $\dim_F R < \infty$ the linear trans T_r must be onto. In particular, $\exists s \in R$ with $T_r(s) = 1$, i.e. $r \cdot s = 1$. So r is a unit. $\square$

Any invariant of a linear trans gives an invariant of $r \in R$. The matrix of $T_r : R \to R$ depends on the choice of basis, but things like its det, tr, char poly do not.

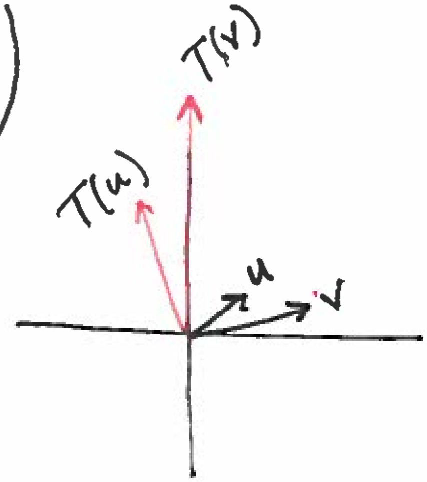
<u>Ex</u>: $F = \mathbb{R}$, $R = \mathbb{C}$, $r = 1+2i$, $T_r : \mathbb{C} \longrightarrow \mathbb{C}$

[Mention geometric meaning.]

matrix wrt to $\{1, i\}$
is $\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$



matrix w.r.t. $\{\underset{u}{1+i}, \underset{v}{2+i}\}$ is $\begin{pmatrix} 7 & 10 \\ -4 & -5 \end{pmatrix}$



as $T_r(1+i) = -1+3i = 7u - 4v$
$T_r(2+i) = 5i = 10u - 5v$

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

In general, for $z = a+bi$, have

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

$$\operatorname{tr} T_z = 2a = 2\,\mathrm{Re}(z)$$

Q: What is the minimal poly of $r = 1+2i$ in $\mathbb{R}[x]$?

Need some poly that has r as a root. Set $M = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$

The char poly of M is $\det(xI - M) = \begin{pmatrix} x-1 & +2 \\ -2 & x-1 \end{pmatrix}$

$= x^2 - 2x + 5$. Now any matrix satisfies

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

As $r \mapsto M$ under our embedding $\mathbb{C} \longrightarrow M_2(\mathbb{R})$

must have $r^2 - 2r + 5 = 0$. As $x^2 - 2x + 5$

has no real roots, it is irred and so

$$m_{r,\mathbb{R}}(x) = x^2 - 2x + 5.$$