Lecture 11: Multiplication in rings as linear transformations

Last time: \( F \subseteq K_1, K_2 \subseteq L \)

Composition: \( K_1 K_2 = \) smallest subfield of \( L \) containing \( K_1 \) and \( K_2 \).

Thm: \([K_1 K_2 : F] \leq [K_1 : F][K_2 : F]\)

[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, \( R = F[[t]] = \{ \sum_{n=0}^{\infty} a_n t \mid a_n \in F \} \)

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

\[
\begin{align*}
f(r_1 + r_2) &= fr_1 + fr_2 \\
(f_1 + f_2)r &= f_1 r + f_2 r \\
f_1(f_2 r) &= (f_1 f_2)r \\
1_F r &= r \quad \text{due that } 1_F = 1_R \text{ since } R \text{ is an integral domain.}
\end{align*}
\]

Contrast: \( R = IR \times IR \)

\[
F = IR \times \{0\} \quad 1_F \cdot (0,2) = (0,0).
\]
Fix $r \in \mathbb{R}$. Then $T: \mathbb{R} \rightarrow \mathbb{R}$ is an $F$-linear transformation as

$$T(rs) = rf s = f(rs) = f(T(s))$$

and

$$T(s_1 + s_2) = r(s_1 + s_2) = rs_1 + rs_2.$$

**Ex:** $F = \mathbb{R}, R = \mathbb{C}, r = 1 + 2i, \ T_r: \mathbb{C} \rightarrow \mathbb{C}$

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

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

$T_r(i) = i - 2 = (-2, 1)$

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

$$\mathbb{C} \rightarrow M_2(\mathbb{R}) \xleftarrow{\text{ring of 2x2 matrices with } \mathbb{R} \text{ entries}}$$

$r \mapsto \text{Matrix of } T_r$

is a ring homomorphism!
That is, \( \{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \} \) is a subring of \( M_2(\mathbb{R}) \) which is isomorphic to \( \mathbb{C} \). In particular,

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

\( \leftarrow \text{cor. to i.} \)

Generalizing, get if \( \dim_F R = n < \infty \), then picking a basis \( r_1, \ldots, r_n \) gives a ring homomorphism:

\[
R \rightarrow M_n(F)
\]

\( r_i \rightarrow \text{matrix of } T_r \text{ with respect to} \)

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 usefulness.]

\[\text{Thm: } R \text{ int domain containing a field } F. \text{ If } \dim_F R < \infty, \text{ then } R \text{ is a field.}\]

\[\text{Pf: Let } r \neq 0 \text{ in } R \text{ and consider } T_r : R \rightarrow R. \text{ As } s \rightarrow rs\]

\( \text{noted above, } \ker T_r = \{0\} \text{ and so as } \dim_F R < \infty \text{ the linear trans } T_r \text{ must be onto. In particular,}\)

\( \exists s \in R \text{ with } T_r(s) = 1, \text{ i.e. } r \cdot s = 1. \text{ So } r \text{ is a unit.} \)
Any invariant of a linear transformation gives an invariant of \( \tau \in \mathbb{R} \). The matrix of \( \tau : \mathbb{R} \rightarrow \mathbb{R} \) depends on the choice of basis, but things like its \( \det, \text{tr}, \text{char} \) polynomials do not.

**Example:** \( F = \mathbb{R} \), \( R = \mathbb{C} \), \( \tau = 1+2i \), \( \tau : \mathbb{C} \rightarrow \mathbb{C} \)

Matrix w.r.t. \( \{1, i\} \) is

\[
\begin{pmatrix}
1 & -2 \\
2 & 1
\end{pmatrix}
\]

Matrix w.r.t. \( \{1+i, 2+i\} \) is

\[
\begin{pmatrix}
7 & 10 \\
-4 & -5
\end{pmatrix}
\]

As \( \tau (1+i) = -1+3i = 7u-4v \)
\( \tau (2+i) = 5i = 10u-5v \)

\( \det \tau = 1+2\cdot2 = 5 = -35+40 \).

In general, for \( z = a+bi \), have

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

\( \text{tr} T_z = 2a = 2 \text{Re}(z) \)
Q: What is the minimal poly of \( r = 1 + 2i \) in \( \mathbb{R}[x] \)?

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

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

\[ = x^2 - 2x + 5. \] 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 \( \mathbb{C} \to M_2(\mathbb{R}) \)

must have \( r^2 - 2r + 5 = 0 \). As \( x^2 - 2x + 5 \)

has no real roots, it is irreducible and so

\[ M_{\mathbb{R}, \mathbb{R}}(x) = x^2 - 2x + 5. \]