Lecture 11: Multiplication in fields as linear transformations

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

Compositum: \( K_1 K_2 = \text{smallest subfield of } L \) containing \( K_1 \) and \( K_2 \).

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

[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 \( T : K \rightarrow K \) is an \( F \)-linear transformation: \( T(f \cdot s) = r f s = f r s = f \cdot T(s) \) 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 \( T_r : \mathbb{C} \rightarrow \mathbb{C} \) with respect to the \( \mathbb{R} \)-basis \( \{1, i\} \) is \[
\begin{pmatrix}
1 & -2 \\
2 & 1 \\
\end{pmatrix}
\] since \[
T_r(1) = 1 + 2i = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \quad \text{and} \quad T_r(i) = -2 + i = \begin{pmatrix} -2 \\ 1 \end{pmatrix}
\]
More generally, the matrix for $T_r$ with $r = a + bi$ is $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$. \[\text{ring of } 2 \times 2 \text{ matrices with } \mathbb{R} \text{ entries}\]

**Claim:** $\mathbb{C} \rightarrow M_2(\mathbb{R})$ is a ring homomorphism.

\[r \rightarrow [T_r]_B\] with $B = \{1, i\}$

**Pf:** \[\{S: \mathbb{C} \rightarrow \mathbb{C} \mid \mathbb{R}-\text{linear}\} \xrightarrow{\cong} M_2(\mathbb{R})\]

\[S \rightarrow [S]_B\]

takes composition of linear maps to matrix mult.

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

**Cor:** $\mathbb{C}$ is isomorphic to the subring $\{(a - b) \mid a, b \in \mathbb{R} \}$ of $M_2(\mathbb{R})$. In particular

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

cor to $i$
Thm: Suppose $[K:F] = n < \infty$. An $F$-basis $B$ of $K$ gives a 1-1 ring hom $K \xrightarrow{\psi} M_n(F)$ by $r \mapsto [Tr]_B$. [Point out usefulness.]

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

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

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

$\rightarrow$ \[ \text{[Note } Tr \text{ rotates and dilates] } \]

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

Since $Tr(u) = -1 + 3i = 7u - 4v$ \quad $Tr(v) = 5i = 10u - 5v$

Then $\det Tr = 1 + 2 \cdot 2 = -35 + 40 = 5$
For \( z = a + bi \), have
\[
\det T_z = \det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a^2 + b^2 = |z|^2
\]
\[
\text{tr } T_z = \text{tr } \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = 2a = 2\Re(z)
\]
For a general \( K/F \), \( \det T_r \) is the norm \( N_{K/F}(r) \).

Q: 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:
\[
M^2 - 2M + 5 \cdot I = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}
\]
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 irreducible.
and hence \( M_r, \mathbb{R}(x) \).
Any \( M \) in \( M_2(\mathbb{R}) \) has char poly \( x^2 - (\text{tr } M)x + \det M \)
So \( z \in \mathbb{C} \setminus \mathbb{R} \) has \( M_z, \mathbb{R}(x) = x^2 - (2\Re(z))x + |z|^2 \).
Ex: D square-free integer \( K = \mathbb{Q}(\sqrt{D}) \)
\( F = \mathbb{Q} \)

Then with \( B = \{1, \sqrt{D}\} \) get \( [T_{a+b\sqrt{D}}]_B = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} \)
and \( N_{K/F}(a+b\sqrt{D}) = a^2 - b^2D \)

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