Decomposing matrices and factoring minimal polynomials

We saw before, that, if A is diagonalizable

$$\begin{bmatrix} \lambda_1 & & & & \\ & \lambda_2 & & & \\ & & \lambda_3 & & \\ & & & \ddots & \\ & & & & \lambda_n \end{bmatrix}$$

then $\chi_A(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$.

Conversely, if $\chi_A(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$ with the λ_i distinct, then A is diagonalizable.

More generally, if A is block diagonalizable:

$$\begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_r \end{bmatrix}$$

then

$$\chi_A(x) = \chi_{B_1}(x)\chi_{B_2}(x)\cdots\chi_{B_r}(x).$$

We'd like a converse again: If $\chi_A(x) = f_1(x)f_2(x)\cdots f_r(x)$, we want to block diagonalize A with blocks corresponding to the factors.

Here is the result we are heading for:

The Primary Decomposition Theorem: If $\chi_A(x)$ factors as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$, then we can block diagonalize A with blocks B_1, B_2, $\ldots$, B_r such that $\chi_{B_i}(x) = f_i(x)$.

Here is the result we are heading for:

The Primary Decomposition Theorem: If $\chi_A(x)$ factors as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$, then we can block diagonalize A with blocks B_1, B_2, $\ldots$, B_r such that $\chi_{B_i}(x) = f_i(x)$.

Note: We proved that factorizations in $F[x]$ are unique, so GCD makes sense.

Here is the result we are heading for:

The Primary Decomposition Theorem: If $\chi_A(x)$ factors as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$, then we can block diagonalize A with blocks B_1, B_2, ..., B_r such that $\chi_{B_i}(x) = f_i(x)$.

More abstract formulation: Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. Let $\chi_A(x)$ factor as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$. Then there are subspaces W_1, W_2, ..., W_r such that $V = \bigoplus W_i$, the transformation T takes W_i to W_i, and $\chi_{T|_{W_i}}(x) = f_i(x)$.

Here is the result we are heading for:

The Primary Decomposition Theorem: If $\chi_A(x)$ factors as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$, then we can block diagonalize A with blocks B_1, B_2, ..., B_r such that $\chi_{B_i}(x) = f_i(x)$.

More abstract formulation: Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. Let $\chi_T(x)$ factor as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$. Then there are subspaces W_1, W_2, ..., W_r such that $V = \bigoplus W_i$, the transformation T takes W_i to W_i, and $\chi_{T|_{W_i}}(x) = f_i(x)$.

This just says "there are W_i", but there is a very precise description: $W_i = \mathrm{Ker}(f_i(A))$.

Here is the result we are heading for:

The Primary Decomposition Theorem: If $\chi_A(x)$ factors as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$, then we can block diagonalize A with blocks B_1, B_2, $\ldots$, B_r such that $\chi_{B_i}(x) = f_i(x)$.

More abstract formulation: Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. Let $\chi_T(x)$ factor as $f_1(x)f_2(x)\cdots f_r(x)$, with $\mathrm{GCD}(f_i, f_j) = 1$. Let $W_i = \mathrm{Ker}(f_i(A))$. Then $V = \bigoplus W_i$, the transformation T takes W_i to W_i, and $\chi_{T|_{W_i}}(x) = f_i(x)$.

It's not just for characteristic polynomials. Here is the version we will prove:

Final version: Let V be a finite dimensional vector space and let $T : V \to V$ be a linear transformation. Let $g(x)$ be a nonzero polynomial with $g(T) = 0$, and let $g(x)$ factor as $f_1(x)f_2(x)\cdots f_r(x)$ with $\mathrm{GCD}(f_i, f_j) = 1$. Let $W_i = \mathrm{Ker}(f_i(T))$.

Then $V = \bigoplus W_i$ and the transformation T takes W_i to W_i.

Moreover, if $g(x) = \chi_T(x)$, then $\chi_{T|_{W_i}}(x) = f_i(x)$. If $g(x) = m_T(x)$, then $m_{T|_{W_i}}(x) = f_i(x)$.