

Abelian groups & The mult. groups of finite fields

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i} \cong \mathbb{Z}^k \oplus \mathbb{Z}/a_1 \oplus \mathbb{Z}/a_2 \oplus \dots$$

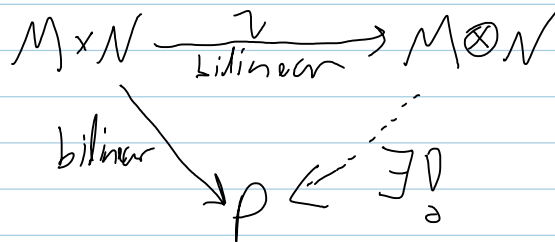
$a_1 | a_2 | a_3 \dots$

Theorem If F is finite, F^* is cyclic.

Proof otherwise, $x^{a_1}-1$ has too many roots.

(Aside: λ is a root of $f \in F[x] \Leftrightarrow x-\lambda | f$, so f may have at most $\deg(f)$ roots)

Theorem. The universal property for tensor products.



Cayley-Hamilton. Let R be any commutative ring, let $A \in M_{n \times n}(R)$, let $\chi_A(t) = \det(tI - A) \in R[t]$. Then $\chi_A(A) = 0$.

Proof I. Substitute $t=A$, so

$$\chi_A(A) = \det(A \cdot I - A) = \det(0) = 0.$$

$$\left[\begin{array}{l}
 \text{tr}(tI - A) = nt - \text{tr} A \\
 \text{so } nA - (\text{tr} A)I = 0 \\
 \text{so all matrices are diagonal } \Downarrow
 \end{array} \right]$$

Proof II. Recall that every matrix B has an "adjoint" B^* s.t. $B^*B = BB^* = \det(B) \cdot I$. Then

$$\begin{array}{l}
 (tI - A)^* (tI - A) = \chi_A(t) I \\
 \parallel \\
 \sum B_k t^k
 \end{array}
 \quad \text{as elements of } M_n R[t] \text{ \& } \text{even } C_A[t], \text{ where } C_A = \{B : AB = BA\}$$

There is a well-defined $\chi_A: C_A[t] \rightarrow C_A[t]$. Applying to both sides, get

$$\left(\sum B_k A^k\right) \cdot (A - A) = \chi_A(A) \cdot I \quad \square$$
