Miscellaneous Algebra Results

Thm/ (Morita Equivalence) Let R be a ring w/ 1.

The left (resp. right) ideals of the matrix ring $M_n(R)$ are in 1-to-1 correspondence w/ the submodules of the free left (resp. right) R-module R^n of rank n.

Def/ A <u>prime ring</u> is a ring R w/ 1 s.t. 0 is a prime ideal in the noncommutative sense; namely, $[IJ \subset 0 \Rightarrow I \subset 0 \text{ or } J \subset 0]$ where I and J are two-sided ideals of R.

Equivalent Definitions:

(i) $[arb = 0 \ \forall r \in R \implies a = 0 \text{ or } b = 0]$.

(ii) All left (resp. right) ideals of R are faithful as left (resp. right) R-modules.
(Hence the Jacobson radical vanishes.)

Def/ A field extension $k \subset F$ is radical if it is obtained as $k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \alpha_2, \ldots, \alpha_n) = F$ for some $\alpha_1, \ldots, \alpha_n \in F$ satisfying $\alpha_i^{m_i} \in k(\alpha_1, \ldots, \alpha_{i-1})$ for some positive integer m_i.

Def/ A Galois extension is solvable if its Galois group is a solvable group.

Thm/ Let k be a field of characteristic zero. Let $k \subset F$ be a Galois extension. Then the extension $k \subset F$ is solvable iff it is contained in a radical extension.

Thm/ (N/C Theorem) G finite group. $H < G$.

$$N_G(H) / C_G(H) < \mathrm{Aut}(H).$$

Thm/ G finite. H Sylow subgroup.

$$\left| G/N_G(H) \right| = \# \text{ copies of } H \text{ in } G.$$

Thm/ (Diamond Isomorphism Theorem).

G finite group. $A \trianglelefteq G$. $B < G$.

Then $AB < G$, $A \cap B \trianglelefteq B$, and

$$[AB : A] = [B : A \cap B].$$

$$\begin{tikzcd}[column sep=small]
 & AB \arrow[dl, equal, "n"'] \arrow[dr, dash] & \\
A \arrow[dr, dash] & & B \arrow[dl, equal, "n"] \\
 & A \cap B &
\end{tikzcd}$$

Thm/ Let $q = p^m$ and let $\mathbb{F}_q$ be a finite field.

Suppose we are interested in computing the (monic) irreducible polynomials of degree d in $\mathbb{F}_q[X]$.

This theorem gives an algorithm for computing such irreducible polynomials.

Let $f_n \in \mathbb{F}_q[X]$ be the polynomial

$$f_n(X) = X^{q^n} - X.$$

(e.g. when $n=1$ this is the polynomial whose splitting field is $\mathbb{F}_q$.)

Then $f_n(X)$ factors as the product of <u>all</u> the monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree d, as d varies over the divisors of n.

(e.g. when $n=1$, $f_1(X) = X^q - X = X^{p^m} - X$ factors completely into degree 1 poly's.)

---

example/ ($p = 2$, $m = 1$) (irred poly's in $\mathbb{F}_2[X]$)

<u>$d=1$</u> : $\quad n = 1 \Rightarrow X^2 - X = X(X-1)$.

So $\{X, X-1\}$ are the irred poly's of deg 1 in $\mathbb{F}_2[X]$.
(obviously)

$d=2$: $n=2$. $\Rightarrow x^4 - x$.

$$
\begin{array}{r|l}
 & x^2 + x + 1 \\
\hline
x^2 - x & x^4 - x \\
 & \underline{x^4 - x^3} \\
 & x^3 - x \\
 & \underline{x^3 - x^2} \\
 & x^2 - x \\
 & \underline{x^2 - x} \\
 & 0
\end{array}
$$

So $\{x^2+x+1\}$ is the only irred poly of deg 2 in $\mathbb{F}_2[x]$. (not so obvious!)

$d=3$: $n=3$. $\Rightarrow x^8 - x$.

$$
\begin{array}{r|l}
 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\hline
x^2 - x & x^8 - x
\end{array}
$$

An irred poly of deg 3 must have no roots. (and in fact this is sufficient.)

They are $\{x^3+x^2+1,\ x^3+x+1\}$.

Indeed, $(x^3+x^2+1)(x^3+x+1) = x^6+x^4+\cancel{x^3}+x^5+\cancel{x^3}+x^2+x^3+x+1$

$= x^6+x^5+x^4+x^3+x^2+x+1$

Thm/ $Aut_{F_p}(F_{p^d})$ is cyclic, and is generated by the Frobenius map $X \mapsto X^p$ (which is an iso in this case).

Thm/ If F_{p^d} is a finite field, then $(F_{p^d})^{\times}$ is a cyclic multiplicative group, of order $\phi(p^d) = p^d - 1$.

Thm/ If q is a prime and if F_{p^n} contains a primitive q^{th} root of unity, then every $a \in F_{p^n}$ has a q^{th} root in the unique extension $F_{p^{nq}}$ of degree q over F_{p^n}.

Note: If $q \mid p^n - 1$, then F_{p^n} has a primitive q^{th} root of unity.

Thm/ If A is a f.d. (or algebraic) integral domain that is an algebra over F, an alg closed field, then $A = F$.

Thm/ (Extension Theorem) Let $\varphi : K_1 \to K_2$ be an isomorphism of fields. Let $\{f_i\}_{i=1,\dots,n}$ be a collection of polynomials in $K_1[x]$ and set $g_i = \varphi(f_i)$, $i=1,\dots,n$. If L_1 is a splitting field of $\{f_i\}$ over K_1 and L_2 is a splitting field of $\{g_i\}$ over K_2, then there is an isomorphism $L_1 \to L_2$ extending the isomorphism $\varphi : K_1^{\subset L_1} \to K_2^{\subset L_2}$.

Cor/ Let $f \in k[x]$ be separable irred and let L be the splitting field of f over k w/ roots $\alpha_1, \dots, \alpha_n$ where $n = \deg f$. Then for every α_i, α_j, $i \neq j$, there is an iso $k(\alpha_i) \xrightarrow{\varphi} K(\alpha_j)$ over k which extends to an auto $\tilde{\varphi} \in \operatorname{Aut} L/K$.

Def/ The Galois group of a separable polynomial $f \in K[x]$ over K is the Galois group of the Galois extension L/K where L is the splitting field of f over K.

Cor/ The Galois group of a separable irreducible poly $f \in K[x]$ over K is a transitive subgroup of S_n where $n = \deg f$.

Here: A subgroup H of S_n is transitive if the action of H on $\{1, \ldots, n\}$ is transitive.

Fact/ • The transitive subgroups of S_3 are A_3 and S_3.

• The transitive subgroups of S_4 are $S_4, A_4, D_8, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4$.

Thm/ Over characteristic 0 or finite fields, an irreducible polynomial is always separable.

Maschke's theorem

Let G be a finite group and let K be a field of characteristic 0. Then the group algebra $K[G]$ is semisimple.

Cor/ Take $k = \mathbb{C}$ in Maschke's thm.

Then $K[G] \cong \prod_{i=1}^{r} M_{n_i}(\mathbb{C})$ where r is the number of irreducible representations of G = the number of conjugacy classes of G, and n_i is the degree of the i^{th} irreducible representation.

(adapted from Malikov)

Thm/ Let A be an Artinian algebra over a field F. Then

$$A \cong \prod_{i=1}^{n} (A_i, m_i)$$

is a product of local Artinan algebras.

If in addition A is Noetherian, then

$$m_i^{n_i} = 0 \text{ for some power } n_i.$$

If A is Artinian and affine (i.e. $A \cong F[x_1, \dots, x_n]/J$ is the quotient of a polynomial ring over an alg closed field F and has no nilpotent elements), then each $(A_i, m_i) \cong F$ hence $A \cong F \times F \times \cdots \times F$ is a product of fields.

(Important Rmk: (A_i, m_i) is isomorphic to the localization A_{m_i} of A at some max ideal m_i.)

Thm/ Let R be a comm ring w/ 1. Let M be an R-module.

The covariant functor $\_\_ \otimes_R M$ is right exact.

The contravariant functor $\mathrm{Hom}_R(M, -)$ is left exact.

M is flat iff $\_\_ \otimes_R M$ is exact.

M is proj iff $\mathrm{Hom}_R(M, -)$ is exact.

Nakayama lemma/ If (R, M) is a local ring and if N is a f.g. R-module s.t. $M \cdot N = 0$, then $N = 0$.

Thm/ (Nullstellensatz) (adapted from Aluffi)

k field. If F/k is a field extension that is finitely generated over k, then it is a finite extension. If k is alg closed, then $F \cong k$.

Cor/ k field. If m is a maximal ideal of $k[X_1, \ldots, X_n]$, then $k[X_1, \ldots, X_n]/m$ is a finite field ext over k.

(adapted from Aluffi)

Def/ A field extension $k \subset F$ is separable if the minimal polynomial $m_\alpha(X) \in k[X]$ is separable for all $\alpha \in F$.

Def/Thm/ Let $k \subset E$ be an algebraic ext. The number of extensions $E \subset \overline{k}$ of E into the algebraic closure of k extending $k \subset \overline{k}$ is called the <u>separability degree of $k \subset E$</u> denoted $[E:k]_s$.

Then always $[E:k]_s \geq 1$.

If E/k is finite, then $[E:k]_s \leq [E:k]$, with equality if and only if E/k is separable.

7

Lemma/ (adapted from Aluffi)

a, b positive integers.

Then $x^a - 1$ divides $x^b - 1$ iff a divides b.