ALGEBRA QUALIFYING EXAM SPRING 2012

Work all of the problems. *Justify the statements in your solutions by reference to specific results*, as appropriate. Partial credit is awarded for partial solutions. The set of rational numbers is Q and set of the complex numbers is C.

1. Let I be an ideal of $R = C[x_1, \ldots, x_n]$. Show that $\dim_C R/I$ is finite $\Leftrightarrow$ I is contained in only finitely many maximal ideals of R.

   $\Rightarrow$ ✓ ? $\Leftarrow$ Nullstellensatz

2. If G is a group with $|G| = 7^2 \cdot 11^2 \cdot 19$, show that G must be abelian and describe the possible structures of G.

   sylow.

3. Let F be a finite field and G a finite group with GCD{*char F*, $|G|$} = 1. The group algebra $F[G]$ is an algebra over F with G as an F-basis, elements $\alpha = \sum_G a_g g$ for $a_g \in F$, and multiplication that extends $ag \cdot bh = ab \cdot gh$. Show that any $x \in F[G]$ that is not a zero left divisor (i.e. if $xy = 0$ for $y \in F[G]$ then $y = 0$) must be invertible in $F[G]$.

   Maschke + Artin Wedd.

4. If $p(x) = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in Q[x]$ and if $Q \subseteq M \subseteq C$ is a splitting field for $p(x)$ over Q, argue that Gal(M/Q) is solvable.

   solvable by radicals.

5. Let R be a commutative ring with 1 and let $x_1, \ldots, x_n \in R$ so that $x_1y_1 + \cdots + x_ny_n = 1$ for some $y_j \in R$. Let $A = \{(r_1, \ldots, r_n) \in R^n \mid x_1r_1 + \cdots + x_nr_n = 0\}$. Show that $R^n \cong_R A \oplus R$, that A has n generators, and that when $R = F[x]$ for F a field then A_R is free of rank $n - 1$.

   canonical $\pi_A : R \oplus A \xrightarrow{R^n} A$. map is injective. proj. modules over PID

6. For p a prime let F_p be the field of p elements and K an extension field of F_p of dimension 72.
   i) Describe the possible structures of $Gal(K/F_p)$.
   ii) If $g(x) \in F_p[x]$ is irreducible of degree 72, argue that K is a splitting field of $g(x)$ over F_p.
   iii) Which integers $d > 0$ have irreducibles in $F_p[x]$ of degree d that split in K?

   galois

spring 2012

① $I \subseteq R = \mathbb{C}[x_1 \dots x_n]$

Show R/I has finite dim over $\mathbb{C} \Leftrightarrow I$ is contained in finitely many max ideals.

$(\Rightarrow)$ R-ring $\Rightarrow$ R/I ring w/ $\dim_{\mathbb{C}} R/I < \infty$.

Thus R/I is artinian & commutative (since R is commutative) and thus has finitely many max ideals.

Hence by the correspondence theorem $\exists$ only finitely many max ideals $I \subseteq M \subseteq R$. $\Rightarrow$ $I \subseteq \bigcap_{\alpha=1}^{k} M_\alpha$; $k < \infty$.

$(\Leftarrow)$ Now suppose $I \subseteq \bigcap_{\alpha}^{k} M_\alpha$; M_α - maximal.

Then, in $R \Rightarrow M_\alpha = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ so $Var(M_\alpha) = \{a_\alpha\} \subseteq \mathbb{C}^n$.

~~In particular $Var(I) = \cup a_i = \cup Var(M_i) = Var(\cap M_i)$~~

~~$\Rightarrow$ Note that if $I \subseteq \bigcap^{k} M_\alpha \Rightarrow \sqrt{I} \subseteq \bigcap^{k} M_\alpha$ since by nullstellensatz~~

~~$I \subseteq \sqrt{I} = Id(var(I)) \subseteq Id(\bigcap^{k} M_\alpha) = \bigcap^{k} M_\alpha$, so WLOG, suppose $I = \sqrt{I}$.~~

~~Then, $Id(Var(I)) = Id(var(\cap M_i)) = \bigcap^{k} M_i$~~

Note that if $I \subseteq \bigcap^{k} M_\alpha \Rightarrow \sqrt{I} \subseteq \bigcap^{k} M_\alpha$ by Nullstellensatz since $Id(var(\bigcap^{k} M_\alpha)) = \bigcap^{k} M_\alpha$

so WLOG take $I = \sqrt{I}$.

Then recall that Max ideal in $\mathbb{C}[x \dots x_n] \overset{bij}{\Longleftrightarrow}$ pts in $\mathbb{C}^n$.

Furthermore $Var(I) = \{a_1 \dots a_n\} = Var(\cap M_\alpha)$ - var max ideals containing I. $< \infty$.

Thus $R/I = R/Id(Var(I)) = R/Id(\{a_i\}) = R/Id(Var(\bigcap^{k} M_i)) = R/\bigcap^{k} M_i$

now each M_i is prime & disjoint from each other, & since $\bigcap^{k}$ is finite then

$R/\bigcap^{k} M_i \simeq R/\prod^{k} M_i \overset{\text{Chinese Rem. thm.}}{=} \prod^{k} R/M_i \simeq \prod^{k} \mathbb{C} \simeq \mathbb{C}^k$. w/ $k < \infty$. since $R/M_i \simeq \mathbb{C}$ for M_i are maximal.

Spring 2012

② $|G| = 7^2 \cdot 11^2 \cdot 19$

G is abelian and describe structure

Pf $n_{19} \equiv 1 \bmod 19$ & $n_{19} = 1, \cancel{7}, \cancel{11}, \cancel{7^2}, \cancel{11^2}, \cancel{7 \cdot 11}, \cancel{7 \cdot 11^2}, \cancel{7^2 \cdot 11^2}$

$n_{11} \equiv 1 \bmod 11$ & $n_{11} = 1, \cancel{7}, \cancel{7^2}, \cancel{19}, 7 \cdot 19, \cancel{7^2 \cdot 19}$

$n_7 \equiv 1 \bmod 7$ & $n_7 = 1, \cancel{11}, \cancel{11^2}, \cancel{19}, \cancel{11 \cdot 19}, \cancel{11^2 \cdot 19}$.

So $n_{19} = 1$ & $n_7 = 1$ $\Rightarrow$ $\exists$ normal subgroup $|PQ| = 19 \cdot 7^2$.

Since $P \cap Q = \phi$ $\Rightarrow$ $PQ \cong P \times Q$ w/ Q - abelian since all grps of order p^2 are abelian. Let R - sylow 11 grp.

So consider $\varphi : R \longrightarrow Aut(P \times Q)$

then if $Q = \mathbb{Z}_7 \times \mathbb{Z}_7$ then $Aut(P \times Q) = Aut(P) \times Aut(Q)$

now $|Aut(P)| = 18$ and $|Aut(Q)| = (p^2 - p)(p^2 - 1) = (p-1)^2(p+1) \cdot p$
$= 6^2 \cdot 8 \cdot 7$

So then since $|R| = 11^2$ $\exists$ some elmt of order 11 in R,

however, $11 \nmid 6^2 \cdot 8 \cdot 7$ & $11 \nmid 18$ $\Rightarrow$ φ must be trivial.

If $Q = \mathbb{Z}/_{7^2}$ $\Rightarrow$ $|Aut(Q)| = 7^2 - 7 = 7(7-1) = 7(6)$

but again $11 \nmid 7 \cdot 6$ $\Rightarrow$ φ is trivial

So $G \simeq R \times (P \times Q)$ which is abelian

w/ $R = \mathbb{Z}/_{11} \times \mathbb{Z}/_{11}$ or $\mathbb{Z}/_{11^2}$

& $Q \simeq \mathbb{Z}/_7 \times \mathbb{Z}/_7$ or $\mathbb{Z}/_{7^2}$

(3) F - finite field, G - finite group w/ $\{ \operatorname{char} F ; |G| \} = 1$.

$F[G] = \{ \sum a_g g ; a_g \in F , g \in G \}$.

Show that any $x \in F(G) \ni xy = 0 \Rightarrow y = 0$ is invertible

Pf Since $\operatorname{char} F \nmid |G| \Rightarrow FG$ is semisimple (Mashke's thm)

so $FG \simeq M_{n_1}(\Delta_1) \times \cdots \times M_{n_k}(\Delta_k)$ by Artin Wedd.

F - finite field, G - finite gp $\Rightarrow FG$ is finite $\Rightarrow \Delta_i = F_i$ - fields$/F$

$FG \simeq M_{n_1}(F_1) \times \cdots \times M_{n_k}(F_k)$

So then given any $x \in FG \Rightarrow x = (a_1, \ldots, a_k)$ w/ $a_i \in M_{n_i}(F_i)$

so then if $a_i \cdot y = 0 \Rightarrow y = 0$ then a_i must be invertible

since if a_i were not invertible then $\exists$ vector $v \ni a_i v = 0$ for $v \neq 0$.

Hence $a_i \cdot [v \ 0 \cdots 0] = 0$ for $y = [v \ 0 \cdots 0] \neq 0$

so a_i must be invertible for $\forall i \Rightarrow x$ is invertible

(4) $p(x) = x^8 + 2x^6 + 3x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$, $\mathbb{Q} \subseteq M \leq \mathbb{C}$ is a splitting field for $p(x)$ over $\mathbb{Q}$, argue $Gal(M/\mathbb{Q})$ is solvable.

Pf let $y = x^2 \Rightarrow p(y) = y^4 + 2y^3 + 3y^2 + 2y + 1$.

Then if E - splitting field of $p(y)$ we have that if α is a root of $p(y)$, then $\pm\sqrt{\alpha}$ is a root of $p(x)$.

So then

$$\begin{array}{l} L = \mathbb{Q}(\sqrt{\alpha}) \\ \quad | \qquad\qquad \Big\} \text{ deg } 2 \\ E = \mathbb{Q}(\alpha) \\ \quad | \\ \mathbb{Q} \end{array}$$

In particular E is the splitting field of a deg. 4 polyn.

$\Rightarrow E$ is solvable by radicals. $\Rightarrow E/\mathbb{Q}$ is solvable ext.

Clearly L/E is also solvable by radicals (by above)

so then since $Gal(L/\mathbb{Q}) / Gal(L/E) \cong Gal(E/\mathbb{Q})$

$\Rightarrow Gal(L/\mathbb{Q})$ is also solvable

⑤ R - com. Ring w/ 1. $\exists \sum x_i y_i = 1$ for some $y_i \in R$.

$A = \{(r_1 \ldots r_n) \in R^n ; \sum x_i r_i = 0\}$, Show $R^n \cong_R A \oplus R$, A has n gen. & when $R = F[x]$, F-field $\Rightarrow A_R$ is free of rank $n-1$.

Pf let $\varphi : R^n \twoheadrightarrow R$, $(r_1 \ldots r_n) \mapsto \sum r_i x_i$. Then $\varphi(y_1 \ldots y_n) = 1$ so φ is surjective and $\operatorname{Ker}\varphi = A$.

So then since R is free, it is projective so that the s.e.s. splits

$$0 \to A \hookrightarrow R^n \twoheadrightarrow R \to 0$$

where $R^n \cong R \oplus A$

Now $\pi : R^n \sim R[x_1 \ldots x_n] \twoheadrightarrow A$ so A has n-generators

and if $R = F[x] \Rightarrow R$ is a PID so by the fund. thm of f.g. mod over PID $\Rightarrow A \cong tA \oplus R^k$

However $R^n \cong A \oplus R \cong tA \oplus R^{k+1} \Rightarrow tA = 0$ & $k+1 = n$, $k = n-1$

so $A \cong R^{n-1} \Rightarrow \dim_R A = n-1$.

⑥ p-prime, K ext of F_p of dim 72. $\Rightarrow$ $K = F_{p^{72}}$

(i) describe structure of $Gal(K/F_p)$

(ii) if $g(x) \in F_p(x)$ irred of deg 72, argue K is a splitting field of $g(x)$ over F_p.

(iii) which integers $d > 0$ have irreducibles in $F_p[x]$ of deg d that split in K.

Pf (i) Since K is a finite ext over a finite field then

$Gal(K/F_p)$ is cyclic $\Rightarrow$ $Gal(K/F_p) = \mathbb{Z}_{72}$

(ii) $g(x)$ irreducible over $\mathbb{F}_p$ $\Rightarrow$ if α is a root then $g(x)$ splits over $\mathbb{F}_p(\alpha)$. But then α - has deg 72, $\Rightarrow$ $[\mathbb{F}_p(\alpha) : F_p] = 72$

since extensions over finite fields are unique $\Rightarrow$ $\mathbb{F}_p(\alpha) = K$.

iii) Now by the same logic if $d \mid 72$ then $\mathbb{F}_{p^d} \subseteq F_{p^{72}}$

so any irreducible of deg $d \mid 72$ will split over $\mathbb{F}_{p^{72}}$.

...