ALGEBRA EXAM FALL 2007

1. Let G be a group of order 105.
   (a) Show G has a normal subgroup of index 3.
   (b) Show $Z(G) \neq 1$.
   (c) Determine all possibilities for G.

2. Let p be a prime. A group G is called p-divisible if the map $x \to x^p$ is surjective. Suppose that G is a finitely generated abelian group. Show that G is p-divisible if and only if G is finite and p does not divide the order of G.

3. Let $R = \mathbb{C}[x_1, \ldots, x_n]$. Suppose that $f \in R$ is irreducible. If $g(a) = h(a)$ whenever $f(a) = 0$, show that $g + (f) = h + (f)$ in $R/(f)$.

4. Let F be a field. Suppose that A is an F-subalgebra of $M_n(F)$ containing the identity of $M_n(F)$.
   (a) If A is a domain, show that A is a division algebra and $\dim A \leq n$.
   (b) If A is simple, show that $(\dim A) | n^2$ (hint: Let V be the space of column vectors of size n over F – this is a left $M_n(F)$-module of dimension n; show that V is a direct sum of say s isomorphic copies of a simple A-module U. Relate the dimension of A and the dimension of U).

5. Let p be a prime. Let $F := \mathbb{F}_{p^n}$ be the field of size of p^n. Let $f(x) \in F[x]$ be irreducible of degree t.
   (a) Show that the splitting field for f has size p^{nt}.
   (b) If $n = 1$, show that $f(x) | (x^{p^m} - x)$ if and only if $t | m$.
   (c) How many irreducible polynomials of degree 6 are there over $\mathbb{F}_2$?

6. Let R be a commutative ring with 1. Assume that $R = a_1 R + \ldots + a_n R$ for some $a_i \in R$. Let $M =: \{(r_1, \ldots, r_n) \in R^n | \sum a_i r_i = 0\}$. Show that M is a projective R-module and can be generated by n elements as an R-module.

Algebra - Fall 2007:

① $|G| = 105 = 3 \cdot 5 \cdot 7$

(a) G has normal s.g. of index 3

Sylow: $r_7 \equiv 1 \pmod 7$ & $r_7 \mid 3 \cdot 5 \Rightarrow r_7 = 1, 15$

$r_5 \equiv 1 \pmod 5$ & $r_5 \mid 3 \cdot 7 \Rightarrow r_5 = 1, 21$

$r_3 \equiv 1 \pmod 3$ & $r_3 \mid 5 \cdot 7 \Rightarrow r_3 = 1, 7$.

Case $r_7 = 1$: Then the Sylow 7-s.g. is normal, call it N

Now choose S a sylow 5-s.g. ; so SN is s.g. of index 3

Now apply repn on cosets: $\exists$ hom $\varphi: G \to S_3$ & $\ker \varphi \subseteq SN$

Now, for $g \in G$, $\varphi(g)$ has the same order; but $\varphi(g) \in S_3$, so can have orders 2 or 3, therefore all order 5 and 7 elts must be in the kernel, hence $SN \subseteq \ker \varphi$

$\Rightarrow \ker \varphi = SN$. $\Rightarrow$ SN normal.

Case $r_7 = 15$: In this case we have $6 \cdot 15 = 90$ order 7 elts.

So then we have $105 - 91 = 14$ possible elts for orders 3 & 5,

hence by counting, $r_5 = 1$ (since cannot be 21), hence the Sylow 5-s.g. is normal; let it be N and let Q be a Sylow 7-s.g. and proceede as before to get QN normal.

(b) Show $Z(G) \neq 1$: see pt(c)

(c) Classify all possible G:

By pt (a), $\exists$ normal s.g. index 3. ; let it be N.

Now let H be order 3 s.g. and we have $G = N \rtimes H$.

So we have homomorphism $\varphi: H \longrightarrow \mathrm{Aut}(N)$ ← cyclic since order 3.

$H = \langle h \rangle$

$\cong \mathrm{Aut}(\mathbb{Z}_5 \oplus \mathbb{Z}_7)$

$\cong \mathbb{Z}_4 \oplus \mathbb{Z}_6$ ← since cyclic.

$h \longmapsto \sigma_h(n) = hnh^{-1} \in n^k$

since $|H|=3$ and φ a homomorphism, $\varphi(h)$ is order 3 or 1.

- <u>case order 1</u>: $\sigma_h(n)=n$, hence $hnh^{-1}=\sigma_h(h)=n$

  $\Rightarrow G$ abelian $\Rightarrow G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$

  (part (b): clearly $Z(G)\neq 1$ here)

- <u>Case order 3</u>: Now must find order 3 elts of $\mathrm{Aut}(\mathbb{Z}_5\oplus\mathbb{Z}_7) \cong \mathbb{Z}_4\oplus\mathbb{Z}_6$.

  Letting $\langle c\rangle = \mathbb{Z}_6$, we see there are exactly 2: $(1, c^2)$ and $(1, c^4)$ (no order 3 elts can arise from $\mathbb{Z}_4 = \langle z\rangle$)

  Let $\mathbb{Z}_5 = \langle\alpha\rangle$, $\mathbb{Z}_7 = \langle\beta\rangle$ and $\theta_1 \in \mathrm{Aut}(\mathbb{Z}_5\oplus\mathbb{Z}_7)$

  Then: $\theta_1 : \mathbb{Z}_5\oplus\mathbb{Z}_7 \to \mathbb{Z}_5\oplus\mathbb{Z}_7$, $\alpha, \beta \mapsto \alpha, \beta^2$ $\Rightarrow$ $\theta_1^3(\alpha,\beta) = (\alpha,\beta^8) = (\alpha,\beta) = \mathrm{id}(\alpha,\beta)$

  similarly order 3: $\theta_2 : \mathbb{Z}_5\oplus\mathbb{Z}_7 \to \mathbb{Z}_5\oplus\mathbb{Z}_7$, $\alpha, \beta \mapsto \alpha, \beta^4$ — <u>order 3</u>

  <u>case θ_1</u>: $\sigma_h(\alpha,\beta) = \theta_1(\alpha,\beta) = (\alpha,\beta^2)$

  $\Rightarrow$ $h\alpha h^{-1}=\alpha$, $h\beta h^{-1}=\beta^2$ $\Rightarrow$ $G \cong \langle \alpha,\beta,h : h\alpha h^{-1}=\alpha,\ h\beta h^{-1}=\beta^2,\ \alpha^5=\beta^7=h^3=1\rangle$

  (part (b): $Z(G)\neq 1$)

  <u>case θ_2</u>: $\sigma_h(\alpha,\beta) = \theta_2(\alpha,\beta) = (\alpha,\beta^4)$

  $\Rightarrow$ $h\alpha h^{-1}=\alpha$, $h\beta h^{-1}=\beta^4$ $\Rightarrow$ $G \cong \langle \alpha,\beta,h : h\alpha h^{-1}=\alpha,\ h\beta h^{-1}=\beta^4,\ \alpha^5=\beta^7=h^3=1\rangle$

  hence both are isomorphic

  now note that $(h\beta h^{-1})^2 = (\beta^4)^2 \Rightarrow h\beta^2 h^{-1} = \beta^8 = \beta \Rightarrow \beta^2 = h^{-1}\beta h$

(2) p prime. G is p-divisible if $x \mapsto x^p$ surj.

Show: G fin-gen abelian grp then G p-div $\iff |G| < \infty$ & $p \nmid |G|$.

($\Rightarrow$) G p-div.

By FTOFGAGrp, $G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$

now, $\begin{matrix} G \to G \\ x \mapsto x^p \end{matrix}$ is surjective, i.e.:

$$a \oplus \alpha_1 \oplus \cdots \oplus \alpha_n \longmapsto a^p \oplus \alpha_1^p \oplus \cdots \oplus \alpha_n^p \text{ surjective.}$$

Hence the map is surj. in each coordinate:

- $a \mapsto a^p$, $\mathbb{Z} \to \mathbb{Z}$ is never surjective (unless $p = 1$), hence $n = 0$. $\Rightarrow |G| < \infty$
- $x \mapsto x^p$, $\mathbb{Z}_{p_i^{k_i}} \to \mathbb{Z}_{p_i^{k_i}}$ is only surjective if $p \neq p_i$ since any elt in $\mathbb{Z}_{p_i^{k_i}}$ has order a power of p, hence not injective, hence not surjective since finite.

  hence $p_i \neq p$ for all i $\Rightarrow p \nmid |G|$.

($\Leftarrow$) $|G| < \infty$ & $p \nmid |G|$.

As before, $G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$ & $p \neq p_i$ for all i.

WTS $\begin{matrix} \mathbb{Z}_{p_i^{k_i}} \to \mathbb{Z}_{p_i^{k_i}} \\ x \mapsto x^p \end{matrix}$ is surjective.

if $\langle \alpha \rangle = \mathbb{Z}_{p_i^{k_i}}$, then $\langle \alpha^p \rangle = \mathbb{Z}_{p_i^{k_i}}$ since $\text{ord}(\alpha) = p_i^{k_i}$

and $\gcd(p_i^{k_i}, p) = 1$ $\Rightarrow$ $x \mapsto x^p$ surjective.

(3) $R = \mathbb{C}[x_1, \dots, x_n]$. Suppose $f \in R$ irreducible.
If $g(a) = h(a)$ whenever $f(a) = 0$, show that $g + (f) = h + (f)$ in $R/(f)$.

Suppose $\alpha \in \mathbb{C}^n$ with $f(\alpha) = 0 \Rightarrow g(\alpha) = h(\alpha) \Rightarrow g(\alpha) - h(\alpha) = 0$, hence for $\alpha \in \mathrm{Var}(f)$, $g(\alpha) - h(\alpha) = 0 \Rightarrow g - h \in \mathrm{Id}(\mathrm{Var}(f)) = \sqrt{(f)} = (f)$ and (f) prime since f irreducible, so $g - h \in \sqrt{(f)} = (f)$, hence $g - h = 0$ in $R/(f)$ & thus $g = h$ in $R/(f)$.

(4) F field, $A \subseteq M_n(F)$ an F-subalg w/ identity of $M_n(F)$.

(a) If A domain, show A division alg & $\dim A \leq n$.

$A \subseteq M_n(F)$ F-subalg $\Rightarrow$ A artinian $\Rightarrow$ $J(A)$ nilpotent $\Rightarrow$ $J(A) = 0$ since A is a domain $\Rightarrow$ A is Jacobson s.s.

So A art + Jac s.s. $\Rightarrow$ A semisimple.

By Artin-Wedd, $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$

A is a domain, so each of $n_i = 1$ and each D_i is domain

(5) p prime, $F = \mathbb{F}_{p^n}$, $f \in F[x]$ irreducible & $\deg f = t$.

(a) The splitting field for f has size p^{nt}.

Let E/F be splitting field for f, therefore a finite extension, hence $E = \mathbb{F}_{p^k}$ (since must be larger & same char.) $[E:F]$

Now, since $\mathbb{F}_{p^k} \supseteq \mathbb{F}_{p^n} \supseteq \mathbb{F}_p$, we have $[\mathbb{F}_{p^k} : \mathbb{F}_p] = [\mathbb{F}_{p^k} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p]$

$\Rightarrow [\mathbb{F}_{p^k} : \mathbb{F}_{p^n}] = k/n \Rightarrow n|k$.

Now consider $F[x]/(f)$

F field $\Rightarrow F[x]$ PID, and so since f irred, (f) is prime, hence (f) maximal since $F[x]$ PID. $\Rightarrow F[x]/(f)$ field

$f(x) = a_0 + a_1 x + \cdots + a_t x^t$, hence each member of $F[x]/(f)$ will be represented by a remainder poly of degree $< t$.

ie: $b_0 + b_1 x + \cdots + b_{t-1} x^{t-1} + (f) \in F[x]/(f)$

" a generic element.

Each of these elts are distinct, and since $b_i \in F = \mathbb{F}_{p^n}$, we have $(p^n)^t$ different members of $F[x]/(f)$, i.e.

$|F[x]/(f)| = (p^n)^t \Rightarrow F[x]/(f) \cong \mathbb{F}_{p^{nt}}$ since we showed $F[x]/(f)$ a field. This field is also a splitting field of $x^{p^{nt}} - x$ over $\mathbb{F}_p$. Note that f has root $\alpha = x + (f)$ in $F[x]/(f)$, hence

Hence $f(x) | x^{p^{nt}} - x$ since f min poly for $\alpha / \mathbb{F}_{p^{nt}}$, hence $f(x)$ also

splits into linear factors in $\mathbb{F}_{p^{nt}}$

$\deg f = t$ | $[E:F]$, so $t | \frac{k}{n}$ and $n|k$, so $k = nt$ is the smallest such number with these properties, hence $\mathbb{F}_{p^{nt}}$ minimal.

(b) If $n=1$, show $f(x) \mid (x^{p^m}-x) \iff t \mid m$.

Recall $\deg f = t$, $f \in \mathbb{F}_{p^n}[x]$

Recall that $\mathbb{F}_{p^m}$ is defined as the splitting field for $x^{p^m}-x$.

($\Rightarrow$) $f(x) \mid x^{p^m}-x \Rightarrow (x^{p^m}-x) \subseteq (f)$

$\Rightarrow F[x]/(f) \subseteq F[x]/(x^{p^m}-x) \Rightarrow \mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^m}$ ($n=1$)

($\Leftarrow$) $t \mid m \Rightarrow \mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^m} \Rightarrow F[x]/(f) \subseteq F[x]/(x^{p^m}-x)$ $\rightarrow$ $t \mid m$ by tower law.

$\Rightarrow (x^{p^m}-x) \subseteq (f) \Rightarrow f \mid (x^{p^m}-x)$.

(c) How many irred poly of degree 6 over $\mathbb{F}_2$?

(6) R commutative w/ 1 and $R = a_1R + \cdots + a_nR$ for some $a_i \in R$.
Let $M = \{(r_1, \ldots, r_n) \in R^n : \sum a_i r_i = 0\}$.
Show that M is a projective R-module & is generated by n elts as an R-mod

- we'll show A is a summand of a free module (namely $R^n \cong M \oplus R$).
Define the map $\varphi : R^n \to R$, $(r_1, \ldots, r_n) \mapsto a_1r_1 + \cdots + a_nr_n$, hence $\ker\varphi = M$.

Now, since $R = a_1R + \cdots + a_nR$, $\exists\ y_1, \ldots, y_n$ s.t. $1 = a_1y_1 + \cdots + a_ny_n$,
and therefore $r = r \cdot 1 = r(a_1y_1 + \cdots + a_ny_n) = r\varphi(y_1, \ldots, y_n)$
$= \varphi(ry_1, \ldots, ry_n)$, hence φ is a surjective map.

Therefore, by First Isom Thm, $R^n/M \cong R$

Now consider the short exact sequence:

$$0 \longrightarrow \underbrace{\ker\varphi}_{M} \longrightarrow R^n \xrightarrow{\varphi} R \longrightarrow 0$$

Since R is a free module, hence projective, this sequence splits, i.e. $R^n = M \oplus R$, hence M is projective.

- Now, M has n generators as an R-module $\iff \exists$ surj hom.
$\Psi : R[t_1, \ldots, t_n] \to M$. Since R^n is fin-gen w/ n generators, we already have $\Psi : R[t_1, \ldots, t_n] \twoheadrightarrow R^n$.

Let $\pi_M : M \oplus R \cong R^n \twoheadrightarrow M$ be the projection map, and then $R[t_1, \ldots, t_n] \xrightarrow{\Psi} R^n \cong M \oplus R \xrightarrow{\pi_M} M$, hence $\pi_M \circ \Psi$ surj onto M, hence M is generated by n elts as R-module.