ALGEBRA QUALIFYING EXAM, Fall 2009

Notation: $\mathbb{Q}$ denotes the rational numbers, $\mathbb{R}$ the real numbers, $\mathbb{C}$ the complex numbers, and $\mathbb{F}_p$ the field with p elements, for p a prime.

1. Determine up to isomorphism all groups of order $1005 = 3 \cdot 5 \cdot 67$.

2. (a) Let G be a group of order $2^m k$, where k is odd. Prove that if G contains an element of order 2^m, then the set of all elements of odd order in G is a (normal) subgroup of G.
(Hint: consider the action of G on itself by left multiplication Φ_L, and then consider the structure of the permutations $\Phi_L(x)$, for $x \in G$.)
(b) Conclude from (a) that a finite simple group of even order must have order divisible by 4.

3. Give a brief argument or a counterexample for each statement:
(a) $x^{2^n} + 1 \in \mathbb{Q}[x]$ is irreducible for all positive integers n;
(b) Any splitting field for $x^{13} - 1 \in \mathbb{F}_3[x]$ has 3^{12} elements. (c) $\mathcal{G}al(L/\mathbb{Q})$ for L a splitting field over $\mathbb{Q}$ of $x^5 - 2 \in \mathbb{Q}[x]$ has a normal 5-Sylow subgroup.

4. Let A denote the commutative ring $\mathbb{R}[x_1, x_2, x_3]/(x_1^2 + x_2^2 + x_3^2 + 1)$.
(a) Prove that A is a Noetherian domain.
(b) Give an infinite family of prime ideals of A that are not maximal. → krull dim

5. Let $R = \mathbb{C}[x_1, \ldots, x_n]$, let $A = [a_{ij}] \in M_n(\mathbb{C})$, and choose $b_1, \ldots, b_n \in \mathbb{C}$. For each $i = 1, \ldots, n$, set $L_i = a_{i1}x_1 + a_{i2}x_2 + \cdots a_{in}x_n - b_i \in R$, and consider the ideal $I = (L_1, \ldots, L_n) \subseteq R$.
Prove that R/I is finite-dimensional $\iff$ the matrix A is invertible in $M_n(\mathbb{C})$.

6. Let $R = K[x]$, for K a field, and let M be a finitely-generated torsion module over R. Prove that M is a finite-dimensional K-module.

7. Let G be a finite group and K a field, and consider the group algebra $R = KG$ (that is, R is a K-vector space with basis $\{g \in G\}$, and multiplication determined by the group product $g \cdot H$, for $g, h \in G$).
If G is the dihedral group of order 8, find the dimensions of all of the simple (left) modules for $R = \mathbb{F}_5 G$.
(Hint: remember that KG always has the "trivial representation" $V_0 = Kv$, such that for any $g \in G$, $a \in K$, $ag \cdot v = av$.)

4 1-dim rep'ns over $\mathbb{F}_5$

(one thing left, can't be abelian, so $M_2(\mathbb{F}_5)$.

.Algebra - Fall 69 :

① $|G| = 3 \cdot 5 \cdot 67$

Sylow: $r_3 \equiv 1 \pmod 3$ & $r_3 \mid 5 \cdot 67 \Rightarrow r_3 \in 1, \cancel{5}, 67, \cancel{5 \cdot 67}$
$r_5 \equiv 1 \pmod 5$ & $r_5 \mid 3 \cdot 67 \Rightarrow r_5 \in 1, \cancel{3}, \cancel{67}, 3 \cdot 67$
$r_{67} \equiv 1 \pmod{67}$ & $r_{67} \mid 3 \cdot 5 \Rightarrow r_{67} \in 1, \cancel{3}, \cancel{5}, \cancel{3 \cdot 5}$
$\Rightarrow$ Sylow 67-sg. N is normal.

Now choose Sylow 5-sg. S and consider the s-g. NS; apply rep'n on cosets & $\exists\, \phi : G \to S_3$ ($[G:NS] = 3$) w/ $\ker\varphi \subseteq NS$.
Note that $|G/\ker\varphi| \mid |S_3| = 3!$ & $|G/\ker\varphi| \mid |G| = 3 \cdot 5 \cdot 67$
hence $|G/\ker\varphi| \mid \gcd(3!, 3 \cdot 5 \cdot 67) = 3 \Rightarrow |G/\ker\varphi| = 3 \Rightarrow |\ker\varphi| = 5 \cdot 67$
$\Rightarrow \ker\varphi = NS \Rightarrow$ NS normal. $NS \cap H = 1$ since orders coprime
So now we have $G = NS \rtimes H$ where H a Sylow 3-sg.; now consider the hom: $\varphi : H \to \mathrm{Aut}(NS) \cong \mathrm{Aut}(\mathbb{Z}_{67} \oplus \mathbb{Z}_5) \cong \mathbb{Z}_{66} \oplus \mathbb{Z}_4$
$\langle h \rangle \mapsto \sigma_h(n) = hnh^{-1}$

$|H| = 3$, hence σ_h can be order 1 or 3:
Case order 1; $hnh^{-1} = \sigma_h(n) = n \Rightarrow$ abelian $\Rightarrow G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{67}$.
case order 3: Consider $\mathrm{Aut}(NS) \cong \mathbb{Z}_{66} \oplus \mathbb{Z}_4$; order 3 elts only occur in first summand; let $\langle a \rangle = \mathbb{Z}_{66}$, then we have $(a^{22}, 1)$ $(a^{44}, 1)$
Let $\mathbb{Z}_{67} \oplus \mathbb{Z}_5 = \langle \alpha \rangle \oplus \langle \beta \rangle$; want k such that $k^3 \equiv 1 \pmod{67}$
$\Rightarrow k^3 - 1 \equiv 0 \pmod{67} \Rightarrow (k-1)(k^2+k+1) \equiv 0 \pmod{67} \Rightarrow k^2 + k \equiv 66 \pmod{67}$
$\Rightarrow k(k+1) \equiv 66 \pmod{67} \Rightarrow k = 29$ or 37 ($29^2 = 37 \pmod{67}$)
So we have $\theta_1(\alpha, \beta) = (\alpha^{29}, \beta)$, $\theta_2(\alpha, \beta) = (\alpha^{37}, \beta)$ orders 3 in $\mathrm{Aut}(NS)$
case 1: $h(\alpha, \beta)h^{-1} = \sigma_h(\alpha, \beta) = \theta_1(\alpha, \beta) = (\alpha^{29}, \beta)$
$\Rightarrow G \cong \langle h, \alpha, \beta : h^3 = \alpha^{67} = \beta^5 = 1,\ h\alpha h^{-1} = \alpha^{29},\ h\beta h^{-1} = \beta \rangle$
case 2: Similarly, get: $G \cong \langle h, \alpha, \beta : h^3 = \alpha^{67} = \beta^5 = 1,\ h\alpha h^{-1} = \alpha^{37},\ h\beta h^{-1} = \beta \rangle$
But $(h\alpha h^{-1})^{29} = (\alpha^{37})^{29} \Rightarrow h\alpha^{29}h^{-1} = \alpha$, hence they are $\cong$.

② (a) $|G| = 2^m k$, k odd, G contains elt of order 2^m.
Show that set of elts of odd order is a normal s.g. of G.

If the set of odd order elts is a subgroup then it is clearly normal since order is preserved under conjugation.

Step 1: we will show that a group of order $2^\ell k$ with an elt of order 2^ℓ will have an index 2 s.g.

Consider the left regular rep'n, letting $|G| = n$:

$\phi : G \to S_n$, $g \mapsto \gamma_g(h) = gh$; clearly γ_g has fixed pt $\iff g = e$,

hence γ_g consists of $\frac{|G|}{\text{ord}(g)}$ cycles of length $\text{ord}(g)$

Let $x \in G$ such that $\text{ord}(x) = 2^\ell$; then γ_x is $\frac{|G|}{\text{ord}(x)} = \frac{2^\ell k}{2^\ell} = k$ cycles of length $\text{ord}(x) = 2^\ell$.

Therefore $\gamma_x \notin A_n$ since k odd and even length cycles have odd parity

Now $A_n \trianglelefteq S_n$ and $G \leq S_n$ (if inj.) w/ elt not in A_n,

hence $GA_n \cong S_n \Rightarrow 2 = |S_n/A_n| = |GA_n/A_n| \overset{\text{2nd isom. thm}}{=} |G/G\cap A_n|$,

and therefore $\exists H \leq G$ w/ $H \cong G \cap A_n$ & $[G:H] = 2$.

Step 2:

- Case $m = 1$: $|G| = 2k$, let $g \in G$ have odd order.

Then γ_g consists of $\frac{2k}{\text{ord}(g)}$ (even) cycles of length $\text{ord}(g)$, hence $\gamma_g \in A_n$.

Now let $h \in G$ have even order; then γ_h consists of $\frac{2k}{\text{ord}(h)}$ (odd) cycles of length $\text{ord}(h) \Rightarrow \gamma_h \notin A_n$.

Therefore $G \cap A_n$ = odd order elements.
This is a subgroup, so done.

Case $m>1$: $|G| = 2^m k$; By Step 1, we know that $\exists H \leq G$, $H \cong G \cap A_n$ & $[G:H] = 2$, hence $|H| = 2^{m-1}k$.
We have $x \in G$ with $\mathrm{ord}(x) = 2^m$, hence $x^{2^m} = 1$,
hence $(x^2)^{2^{m-1}} = 1 \Rightarrow \mathrm{ord}(x^2) = 2^{m-1}$

Now consider γ_{x^2}; it has $\frac{2^m k}{2^{m-1}}$ ← even cycles of length $2^{m-1} \Rightarrow \gamma_{x^2} \in A_n \Rightarrow x^2 \in H \cong G \cap A_n$. Therefore $|H| = 2^{m-1}k$ w/ elt order $2^{m-1} \Rightarrow \exists H_1 \leq H$ with $[H:H_1] = 2$ by Step 1. Hence $H_1 = 2^{m-2}k$, and we may proceed by induction to get $H_{m-1} \leq H_{m-2} \leq \cdots \leq H_1 \leq H$ where $|H_{m-1}| = 2k$; by case $m=1$, we get $H_m \leq H_{m-1}$ with $|H_m| = k$, the odd order elts in H_{m-1}, i.e. the odd order elements in $H \cong G \cap A_n$.

Finally, if $g \in G$ is odd order then γ_g consists of $\frac{2^m k}{\mathrm{ord}(g)}$ ← even cycles of length $\mathrm{ord}(g)$, hence $\gamma_g \in A_n$.

Therefore $G \cap A_n \cong H$ contains all odd order elts in G, hence since $H_m \leq H$ has all odd order elts of H, it also has all odd order elts of G, and is a subgroup of G since $H_m \leq H \leq G$.

(b) From (a), conclude that a finite simple grp of even order must have order divisible by 4.

Suppose G finite, simple, even order, but $4 \nmid |G|$, hence $|G| = 2k$ with k odd. By Cauchy, G has elt order 2, hence the odd-order elements form a normal subgroup, which is a contradiction to the simplicity; hence the order of G must have 2 or more factors of 2.

③ T/F

(a) $x^{2^n}+1$ is irreducible for all n

Substitute $x-1$ for x to get:

$$(x-1)^{2^n}+1 = \left(\sum_{i=0}^{2^n-1} \binom{2^n}{i} x^{2^n-i}(-1)^i + 1\right) + 1$$
$$= \sum_{i=0}^{2^n-1} \binom{2^n}{i} x^{2^n-i}(-1)^i + 2,$$

which is irreducible by Eisenstein w/ $p=2$. TRUE

(b) Any splitting field for $x^{13}-1 \in \mathbb{F}_3[x]$ has 3^{12} elts

Let $E/\mathbb{F}_3$ be splitting field. Then $E = \mathbb{F}_{3^k}$.

since E spl. field for $x^{13}-1$, $\exists\, a \in E$ s.t. $a^{13}=1$, i.e. $13 \mid |E^\times| = 3^k - 1$; If $k=3$, then $13 \mid 3^3-1 = 27-1 = 26 \neq 3^{12}$

hence $\mathbb{F}_{3^3}$ contains a 13^{th} rt of 1 and $|\mathbb{F}_{3^3}| = 26 \neq 3^{12}$ FALSE

(c) $L/\mathbb{Q}$ spl. field of x^5-2; $Gal(L/\mathbb{Q})$ has normal Sylow 5-s.g.

Roots of poly are $\omega^i \sqrt[5]{2}$ where $\omega^5 = 1$.

so then $L = \mathbb{Q}(\omega, \sqrt[5]{2})$.

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\omega, \sqrt[5]{2}) \arrow[dl, dash, "5"'] \arrow[dr, dash, "4"] & \\ \mathbb{Q}(\omega) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\sqrt[5]{2}) \arrow[dl, dash, "5"] \\ & \mathbb{Q} & \end{tikzcd}$$

$\Rightarrow |Gal(L/\mathbb{Q})| = 20$

Galois ext, so $\exists$ index 4 normal s.g.

$\hookrightarrow$ index 4 s.g. is order 5

TRUE

④ $A = \mathbb{R}[x,y,z]/\overset{\overset{I}{\parallel}}{(x^2+y^2+z^2+1)}$ commutative ring.

(a) Prove A is a noetherian domain

$\mathbb{R}$ field $\Rightarrow$ $\mathbb{R}$ commutative, noetherian $\Rightarrow$ $\mathbb{R}[x,y,z]$ comm, noeth by Hilbert basis. $\Rightarrow$ $\mathbb{R}[x,y,z]/I$ comm, noetherian.

$x^2+y^2+z^2+1$ irreducible $\Rightarrow$ $(x^2+y^2+z^2+1) = I$ prime ideal

$\Rightarrow$ $\mathbb{R}[x,y,z]/I$ domain

hence noetherian domain.

(b) Give an infinite family of non-maximal prime ideals

⑤ $R = \mathbb{C}[x_1, \ldots, x_n]$; $A = [a_{ij}] \in M_n(\mathbb{C})$, $b_1, \ldots, b_n \in \mathbb{C}$.

For each $i = 1, \ldots, n$, set $L_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n - b_i \in R$ and consider the ideal $I = (L_1, \ldots, L_n) \subseteq R$.

<u>Prove</u>: R/I fin-dim $\iff A \in M_n(\mathbb{C})$ invertible

---

($\Leftarrow$) $A = [a_{ij}] \in M_n(\mathbb{C})$ is invertible. ; let $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$

Let $Ax = b$, i.e.

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \Rightarrow \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n - b_1 \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n - b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

A is invertible, so $Ax = b$ has a unique sol'n $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, i.e. there is a unique vector $(y_1, \ldots, y_n)$ such that $L_i(y_1, \ldots, y_n) = 0 \ \forall L_i$.

Therefore, $Var(I) = Var(L_1, \ldots, L_n) = \{(y_1, \ldots, y_n)\}$, and therefore $Id(Var(I)) = (x_1 - y_1, \ldots, x_n - y_n)$; by Nullstellensatz, $\sqrt{I} = (x_1 - y_1, \ldots, x_n - y_n)$

So then $(x_i - y_i)^{n_i} \in I$ for some n_i for all i; now consider $R/I \cong \mathbb{C}[x_1, \ldots, x_n]/I$, hence in R/I, $x_i^{m_i} = p(x_i)$, p polynomial over $\mathbb{C}$ with $\deg p \le m_i$, hence

$$B = \bigcup_{j=1}^{n} \bigcup_{i=1}^{m_j} \{x_j^{\,i}\} \text{ is } \mathbb{C}\text{-basis of } R/I,$$

hence R/I fin-dim'l in $\mathbb{C}$

($\Rightarrow$) Suppose R/I fin-dim'l $\Rightarrow$ R/I artinian $\Rightarrow$ R/I has finitely many max ideals $\Rightarrow$ there are finitely many pts in $Var(I)$ $\Rightarrow$ Finitely many solutions to $Ax = b$ $\Rightarrow$ Sol'n unique, since A linear, hence A invertible.

(6) $R = K[x]$, K field, M fin-gen torsion module over R.
Prove that M is a fin-dim K-module

K field $\Rightarrow K[x]$ PID, so apply Fund. Thm of Mod/PID.

$M \cong R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_n^{e_n})$ (torsion, so no free part)

$\cong K[x]/(p_1^{e_1}) \oplus \cdots \oplus K[x]/(p_n^{e_n})$

But $K[x]/(p_i^{e_i}) \cong \mathrm{span}_K\{1, x, x^2, \ldots, x^{e_i \deg p_i - 1}\}$

Hence each summand fin-dim over K, hence $\dim_K M < \infty$.

(7) Let $G = D_8$ & $k = \mathbb{F}_5$.
Find the dimensions of all the simple left modules for $R = kG$.

$\mathrm{char}(k) = 5$ & $|G| = 8$, and $5 \nmid 8$. So by Maschke's Theorem, R is semisimple.
Now apply Artin-Wedderburn to get $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r)$
we know $|R| < \infty$, hence $|D_i| < \infty$ $\forall i$, hence by little Wedderburn the D_i are fields, $D_i = F_i$:

Recall that the n_i are the dimensions of the simple kG-modules.

$R \cong M_{n_1}(F_1) \oplus \cdots \oplus M_{n_r}(F_r)$
Since $k \subseteq R$, we have $F_i = k$ for all i, so:
$R \cong M_{n_1}(k) \oplus \cdots \oplus M_{n_r}(k)$.
Recall that $r = \#$ of conjugacy classes in G & $n_1^2 + \cdots + n_r^2 = |G| = 8$
We know D_8 has elts order 1, 2, and 4, so at least 3 conj classes.
Hence $n_1 = 2$ & $n_2 = n_3 = n_4 = n_5 = 1$ or $n_i = 1$ $\forall i$. But kG is not abelian, hence $n_i > 1$ for at least one i.
Hence $n_1 = 2$ & $n_2 = n_3 = n_4 = n_5 = 1$, so dimensions are $\underline{2 \text{ or } 1}$