SOLVED

ALGEBRA QUALIFYING EXAM FEBRUARY 2002

Partial credit is given for partial solutions

1. Describe all groups of order $2 \cdot 31 \cdot 61$ up to isomorphism.

2. Let G be a finite solvable group. If $\langle e \rangle \neq N \lhd G$ and is N minimal (for any $H \lhd G$ with $H \subseteq N$ either $H = \langle e \rangle$ or $H = N$) show that $N \cong \mathbb{Z}_p^k = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$, for p a prime and some $k \geq 1$.

3. For any prime p show that $x^4 + 1 \in F_p[x]$ cannot be irreducible. (F_p is the field of p elements. Note that $p^2 \equiv 1 \pmod 8$ for any odd prime.)

4. Let $f(X) = f(x_1, \ldots, x_n) \in C[x_1, \ldots, x_n] = R$ be irreducible. If $g(X), h(X) \in R$ with $g(\alpha) = h(\alpha)$ for all $\alpha \in C^n$ satisfying $f(\alpha) = 0$, show that the images of $g(X)$ and $h(X)$ in $R/(f(X))$ are equal, that is $g(X) + (f(X)) = h(X) + (f(X))$.

5. Let R be a commutative ring with 1.

   i) Show that R is a Noetherian ring $\Leftrightarrow$ for each maximal ideal M of R the localization R_M at M is a Noetherian ring.

   ii) Show that R is a Noetherian $\Leftrightarrow$ every localization of the polynomial ring $R[x,y]$ at its maximal ideals is Noetherian.

6. If R is a right Artinian algebra over the algebraically closed field F show that R is algebraic over F of bounded degree. That is for some fixed $M > 0$ and any $r \in R$, there is some nonzero $f(x) \in F[x]$ depending on r so that $f(r) = 0$ and $\deg f \leq M$.

$\pi : R \to R_M$

$\pi^{-1}(A) = \pi^{-1}(B)$

$J \subseteq R_M$

$x \in \pi^{-1}(J)$; choose $r \in R$

$\pi(A) = \pi(B)$

$\Rightarrow \pi(x) \in J$

$\Rightarrow r\,\pi(x) \in J$

$\Rightarrow \pi(rx) \in J$

$\Rightarrow rx \in \pi^{-1}(J)$

$\Rightarrow$

Algebra - Spring 2002 :

① $|G| = 2\cdot 31\cdot 61$:

$r_{61} \equiv 1 \pmod{61}$ & $r_{61} | 2\cdot 31 \Rightarrow r_{61} = 1, \cancel{2}, \cancel{31}, 2\cdot 31$

$r_{31} \equiv 1 \pmod{31}$ & $r_{31} | 2\cdot 61 \Rightarrow r_{31} = 1, \cancel{2}, \cancel{61}, \cancel{2\cdot 61} \Rightarrow Q \trianglelefteq G$ the Sylow 31-sg.

$r_2 \equiv 1 \pmod 2$ & $r_2 | 31\cdot 61 \Rightarrow r_2 = 1, 31, 61, 31\cdot 61$

Now choose P a Sylow 61-subgroup. Now PQ is a subgroup of index 2, hence by rep'n on cosets $\exists\ \varphi : G \to S_2$ with $\ker\varphi \subseteq PQ$.

So then $|G/\ker\varphi| \,\big|\, |S_2| = 2 \Rightarrow |G/\ker\varphi| = 2 \Rightarrow \ker\varphi = 31\cdot 61$.

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

So now choose S to be a Sylow 2-subgroup and we have $S \cap PQ = 1$ and $SPQ = G$, hence $G = PQ \rtimes S$ and we get hom: $\varphi : \underset{\langle s\rangle}{\overset{\shortparallel}{S}} \to Aut(PQ) \cong Aut(\mathbb{Z}_{61} \oplus \mathbb{Z}_{31}) \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_{30}$

$\langle s\rangle \mapsto \sigma_s(n) = sns^{-1}$

S order 2, hence $\varphi(s)$ order 1 or 2.

Case order 1: abelian, hence $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{31} \oplus \mathbb{Z}_{61}$ ①

Case order 2: we'll count the order 2 elements in $Aut(PQ) \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_{30}$

Let $\mathbb{Z}_{60} = \langle a\rangle$, $\mathbb{Z}_{30} = \langle b\rangle$. Then $(a^{30}, 1)$, $(1, b^{15})$, (a^{30}, b^{15}) are order 2

Let $\mathbb{Z}_{61} = \langle\alpha\rangle$ & $\mathbb{Z}_{31} = \langle\beta\rangle$ and then consider $\theta_i \in Aut(PQ)$

$\theta_1(\alpha, \beta) = (\alpha^{60}, \beta)$ ← $k^2 \equiv 1 \pmod{61} \Rightarrow k^2 - 1 \equiv 0 \pmod{61}$
$\Rightarrow (k-1)(k+1) \equiv 0 \pmod{61} \Rightarrow k = 60$

$\theta_2(\alpha, \beta) = (\alpha, \beta^{30})$ ← By same logic (also $\alpha^{60} = \alpha^{-1}$, $\beta^{30} = \beta^{-1}$)

$\theta_3(\alpha, \beta) = (\alpha^{60}, \beta^{30})$

Case $\sigma_s = \theta_1$: $G \cong \langle s, \alpha, \beta : s^2 = \alpha^{61} = \beta^{31} = 1,\ s\alpha s^{-1} = \alpha^{-1},\ s\beta s^{-1} = \beta\rangle$ ②

Case $\sigma_s = \theta_2$: $G \cong \langle s, \alpha, \beta : s^2 = \alpha^{61} = \beta^{31} = 1,\ s\alpha s^{-1} = \alpha,\ s\beta s^{-1} = \beta^{-1}\rangle$ ③

Case $\sigma_s = \theta_3$: $G \cong \langle s, \alpha, \beta : s^2 = \alpha^{61} = \beta^{31} = 1,\ s\alpha s^{-1} = \alpha^{-1},\ s\beta s^{-1} = \beta^{-1}\rangle$ ④

② $|G|<\infty$ solvable. If $N \trianglelefteq G$ and N minimal normal, show that $N \cong \mathbb{Z}_p^k$ for prime p & $k \geq 1$.

Consider the commutator subgroup $[N,N] := N' \trianglelefteq N$. We'll show first that $N' \trianglelefteq G$ as well; choose $g \in G$ and $n \in N'$: see that $gng^{-1} \in gN'g^{-1}$, and since $n = n_1 n_2 n_1^{-1} n_2^{-1}$ $(n_1, n_2 \in N)$, we have

$$gng^{-1} = gn_1 n_2 n_1^{-1} n_2^{-1} g^{-1}$$
$$= \underbrace{gn_1g^{-1}}_{a \in N}\underbrace{gn_2g^{-1}}_{b \in N}\underbrace{gn_1^{-1}g^{-1}}_{a^{-1} \in N}\underbrace{gn_2^{-1}g^{-1}}_{b^{-1} \in N} \in N'$$

since $N \trianglelefteq G$

Hence $gN'g^{-1} \subseteq N'$, hence $gN'g^{-1} = N'$ (conj. auto.)

$\Rightarrow N' \trianglelefteq G$, hence $\exists\, N' \leq N$ with $N' \trianglelefteq G$, but N is minimal, so $N' = \langle e \rangle$ or N.

Case $N' = N$: Recall G solvable, so the derived series must end with 1: $G \geq G' \geq G^{(2)} \geq \cdots \geq 1$.

Now, G is solvable, so then $N \trianglelefteq G$ is, but we showed that $N' = N$, hence $N^{(k)} = N$ for all k and thus the derived series doesn't terminate, hence N not solvable; contradiction

Hence $N' \neq N$.

Case $N' = \langle e \rangle$: so N is abelian & finite, hence

$N \cong A_{p_1} \oplus \cdots \oplus A_{p_n}$, A_{p_i} the p_i-primary part. (p_i distinct)

$A_{p_i} \leq N$, so, for $a \in A_{p_i}$, $g \in G$: $gag^{-1} \in N$ since $N \trianglelefteq G$,

but $\mathrm{ord}(gag^{-1}) = \mathrm{ord}(a) = p_i^k \Rightarrow gag^{-1} \in A_{p_i}$

$\Rightarrow A_{p_i} \trianglelefteq G$, contradicting minimality of N.

Hence N must be p-primary (so no proper subsets in p-primary decomposition).

So now $N \cong \mathbb{Z}_{p^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_k}}$.
Suppose $e_i \geq 2$; let $P = \overbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}^{k \text{ times}}$, and then $P \trianglelefteq N$; for $g \in G$, $b \in P$, $gbg^{-1} \in N$ since $N \trianglelefteq G$, but $\operatorname{ord}(gbg^{-1}) = p$, hence $gbg^{-1} \in P$, hence $P \trianglelefteq G$ and contained in N, hence contradicts minimality of N, hence $e_i = 1$. $\forall i$

Therefore $N = \overbrace{\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}^{k \text{ times}} \cong \mathbb{Z}_p^{\,k}$

---

③ p prime, show that $x^4+1 \in \mathbb{F}_p[x]$ cannot be irred.
<u>Hint</u>: $p^2 \equiv 1 \pmod 8$ for any odd prime

<u>Case $p=2$</u>: $x^4+1 = (x+1)^4$, hence not irreducible
<u>Case $p \geq 3$</u>: $p^2 \equiv 1 \pmod 8$ for any odd prime, i.e. $8 \mid (p^2-1) = |\mathbb{F}_{p^2}^\times|$.
So there is an order 8 subgroup of $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}_{p^2-1}$, which is cyclic, hence the s.g. is cyclic, hence there exists $a \in \mathbb{F}_{p^2}^\times$ of order 8, hence x^8-1 factors in $\mathbb{F}_{p^2}$ (since the s.g. $\langle a \rangle$ has all roots).
See that: $x^8-1 = (x^4+1)(x^4-1)$
$$= (x^4+1)(x^2+1)(x^2-1) = (x^4+1)(x^2+1)(x-1)(x+1).$$

Now suppose x^4+1 is irreducible over $\mathbb{F}_p$ and let $E/\mathbb{F}_p$ be its splitting field; $4 \mid [E:\mathbb{F}_p]$, but by previous discussion x^4+1 must split in $\mathbb{F}_{p^2}$ (since x^8-1 does), hence $4 \mid [\mathbb{F}_{p^2}:\mathbb{F}_p] = 2$, a contradiction.

Thus x^4+1 is <u>not</u> irreducible.

④ $f(x) = f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n] = R$ irreducible, and $g(x), h(x) \in R$. Suppose $g(\alpha) = h(\alpha)$ $\forall \alpha \in \mathbb{C}^n$ such that $f(\alpha) = 0$; then show the images of g and h are equal in $R/(f)$.

$\alpha \in \mathbb{C}^n$, $f(\alpha) = 0 \Rightarrow g(\alpha) = h(\alpha) \Rightarrow g(\alpha) - h(\alpha) = 0$; hence for $\alpha \in Var(f)$, we have $g(\alpha) - h(\alpha) = 0$, hence $g - h \in Id(Var(f)) = \sqrt{(f)} = (f)$ since (f) is prime since f is irreducible.

Therefore $g - h \in (f)$, hence $g - h \equiv 0$ in $R/(f)$ $\Rightarrow g = h$ in $R/(f)$.

---

⑤ R commutative w/ 1.

(i) Show: R noeth $\Leftrightarrow$ for each max ideal $M \subseteq R$, R_M is noether.

($\Rightarrow$) R noetherian, $M \subseteq R$ maximal ideal (M max $\Rightarrow M$ prime)

Then $R_M = \left\{ \frac{a}{b} : a \in R, b \in R \setminus M \right\} / \frac{a}{b} \sim \frac{c}{d} \Leftrightarrow \exists s \in R \setminus M$ s.t. $s(ad) = s(bc)$

Consider the canonical map $\pi : R \to R_M$ and ideal $J \subseteq R_M$.

Clearly $\pi(\pi^{-1}(J)) \subseteq J$; now choose $\frac{a}{b} \in J$ ($a, b \in R$) and then $\frac{a}{1} = b\left(\frac{a}{b}\right) \in J \Rightarrow a \in \pi^{-1}(J) \Rightarrow \frac{a}{1} \in \pi(\pi^{-1}(J))$

$\Rightarrow \frac{a}{b} = \left(\frac{1}{b}\right)\left(\frac{a}{1}\right) \in \pi(\pi^{-1}(J))$ since $\pi(\pi^{-1}(J))$ ideal in R_M.

Hence $J \subseteq \pi(\pi^{-1}(J))$, and therefore $J = \pi(\pi^{-1}(J))$.

Furthermore, for $x \in \pi^{-1}(J)$, choose $r \in R$ and see that $\pi(x) \in J \Rightarrow \frac{r}{1}\pi(x) \in J \Rightarrow \pi(rx) \in J \Rightarrow rx \in \pi^{-1}(J)$, hence $\pi^{-1}(J)$ is an ideal.

So if A & B are ideals in R_M such that $\pi^{-1}(A) = \pi^{-1}(B)$, then $\pi(\pi^{-1}(A)) = \pi(\pi^{-1}(B)) \Rightarrow A = B \Rightarrow \pi$ is 1-1 between the families of ideals of each of R and R_M, i.e. any ascending chain of ideals in R_M can be "contracted" (hit w/ π^{-1}) to one in R, which is noetherian, hence it will terminate, and since π 1-1 on ideals, so will in R_M.

($\Leftarrow$) $M \subseteq R$ maximal, R_M noeth (for all such M).

As previously seen, $\pi: R \to R_M$ is 1-1 on ideals, hence R_M noeth $\Rightarrow$ R "noeth" on ideals contained in M (i.e. fin-gen). True for all M, so true for all ideals since each ideal is contained in some max. Hence R is noeth.

(ii) R noeth $\Leftrightarrow$ every localization of $R[x,y]$ at its max ideals is noeth.

($\Rightarrow$) R noeth $\Rightarrow$ $R[x,y]$ noeth
$\Rightarrow R[x,y]_M$ noeth $\forall$ max ideals M by part (i)

($\Leftarrow$) Every localization of $R[x,y]$ at max ideals M is noeth
$\Rightarrow R[x,y]$ is noeth $\Rightarrow$ ~~R is noeth.~~
see then that $\varphi: R[x,y] \to R$, $f(x,y) \mapsto f(0,0)$ has $\ker\varphi = (x,y)$,

hence $R[x,y]/\ker\varphi \cong R$, hence R quotient of noeth ring, hence noeth

(6) R artinian F-algebra, F algebraically closed, R/F algebraic ext.
Show: R/F has bounded degree, i.e. $\exists M > 0$ s.t. for any $r \in R$, $\exists f \in F[x]$ s.t. $f(r) = 0$ & $\deg f \leq M$:

- Case R semisimple: By Art-Wedd $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_m}(D_m)$, D_i division rings. Now R an F-alg, hence $F \subseteq D_i$ for all i. Choose $\alpha \in D_i$ and consider the field extension $F(\alpha)/F$; R/F algebraic, hence α alg over F, hence $F(\alpha) = F$ since F alg. closed. Thus $\alpha \in F$, hence $D_i \subseteq F$, hence $D_i = F$. So now $R \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_m}(F)$.

So now for $a \in R$, $a = a_1 + \cdots + a_m$ and the a_i satisfy $f_i \in F[x]$ of degree n_i by Cayley-Hamilton. So A satisfies:

$$f(x) = \prod_{i=1}^{m} f_i\Big(x - \sum_{j \neq i} a_j\Big), \text{ and } \deg f \leq \sum_{i=1}^{m} \deg f_i = \sum_{i=1}^{m} n_i = M, \text{ bound}$$

· General case $R/J(R)$ is Jacobson s.s. & artinian since R is.

$\Rightarrow R/J(R)$ semisimple.

By the semisimple case, $\exists M$ s.t. $\forall r \in R/J(R)$, $\exists f \in F[x]$ with $\deg f \leq M$ where $f(r) = 0$, i.e. any $r \in R$, $f(r) \in J(R)$

But R is artinian $\Rightarrow J(R)$ nilpotent, so $\exists n$ such that $J(R)^n = 0$, hence $f(r)^n = 0$; but $\deg f^n = Mn$, hence for any $r \in R$ $\exists$ polynomial $g \in F[x]$ w/ $g(r) = 0$ & $\deg g \leq Mn$, hence bounded degree.