ALGEBRA QUALIFYING EXAM SPRING 2006

Work all the problems. Be as explicit as possible in your solutions and justify your statements with specific reference to the results that you use. Partial credit will be given for partial solutions. Let Q denote the field of rational numbers, C the field of complex numbers, and $\mathbf{F}_q$ the finite field of q elements.

✓ 1. Up to isomorphism, describe the groups of order $3\cdot17\cdot19$.

2. i) For p a prime, $q = p^k$, and n a positive integer, describe a condition that guarantees that the multiplicative group $\mathbf{F}_q^* = (\mathbf{F}_q - \{0\}, \cdot)$ contains an element of order n.
   ii) Determine the cardinality of a splitting field L over $\mathbf{F}_3$ of $x^{13} - 1 \in \mathbf{F}_3[x]$, and the structure of $Gal(L/\mathbf{F}_3)$

3. Let $f(x) = (x^3 - 2)(x^3 - 3) \in Q[x]$, $M \subseteq C$ a splitting field over Q for $f(x)$, $G = Gal(M/Q)$, and $\omega \in C$ a primitive cube root of unity.
   i) Show that $\omega \in M$.
   ii) Assume that $3^{1/3} \notin Q(\omega, 2^{1/3}) \subseteq M$, and use this to find the order of G. 36
   iii) Describe how the elements of G act on M. 3·2·3
   iv) Determine the structure of G.

4. In $C[x, y]$ show that for some integer $m \geq 1$, $(3x^2 + 10xy + 3y^2)^m \in (x + y - 2, x^2 + y^2 - 10)$, the ideal of $C[x, y]$ generated by $x + y - 2$ and $x^2 + y^2 - 10$.

5. Let $g_1, g_2, \ldots, g_m, \ldots \in R$, a commutative Noetherian ring with 1, and let I be an ideal of R. Assume that for each i there is $k_i \geq 1$ so that $g_i^{k_i} \in I$. Show that there is a positive integer K so that $g_{i_1} g_{i_2} \cdots g_{i_K} \in I$ for any choices of $g_{i_j} \in \{g_i\}$.

6. Let S be a finite ring so that for each $x \in S$, $x^5 = x$.
   i) Show that S contains no nonzero nilpotent element.
   ii) Show that, up to isomorphism, S is a direct sum of copies of $\mathbf{F}_2$, $\mathbf{F}_3$, and $\mathbf{F}_5$.

$x^2 - \alpha\omega^2 x - \alpha\omega x + \alpha^2$ $\qquad \alpha^3\omega^3 = 2$

$\omega = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$(x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$ $\qquad \frac{\alpha^3\omega^2\cdot\omega}{2} = 1$

$(p-1)(p^{k-1} + p^{k-2} + \cdots + p + 1)$

$= p^k + p^{k-1} + \cdots + p^2 + p - (p^{k-1} + \cdots + 1)$ $\qquad 6^{6^{6^6}}$ $\quad 6^{12}$

$= p^k - 1$

$s\beta^7 s^{-1} = \beta^{11}$

$s\beta^{11} s^{-1} = \beta$

$[\mathbb{F}_{3^k} : \mathbb{F}_3] = k$

$\mathbb{F}_{3^3} = \mathbb{F}_{27}$ $\quad \mathbb{F}_{27}^* = \mathbb{Z}_{26}$ $\quad x^{26} = 1$

$\to x^{13}x^{13} = 1$

order 2

~~$G = N \rtimes S$~~

~~so $\varphi: S \to Aut(N) \cong Aut(\mathbb{Z}_6) \cong \mathbb{Z}_2$~~

$3^2 \cdot 2$

$r_3 \equiv 1 \pmod 3$ + $r_3 \mid 2$

$r_2 \equiv 1 \pmod 2$ + $r_2 \mid 3^2$

$r_2 = 1, 3, 9$

8 ~~order 9 elts~~

elts not order 2 or 1

$\cong \mathbb{Z}_2$

$G/\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Algebra: Spring 2006?

1. $|G| = 3 \cdot 17 \cdot 19$:

Sylow: $r_3 \equiv 1 \pmod 3$ & $r_3 \mid 17\cdot19 \Rightarrow r_3 = 1, \cancel{17}, 19, \cancel{17\cdot19}$

$r_{17} \equiv 1 \pmod{17}$ & $r_{17} \mid 3\cdot19 \Rightarrow r_{17} = 1, \cancel{3}, \cancel{19}, \cancel{3\cdot19} \Rightarrow$ normal

$r_{19} \equiv 1 \pmod{19}$ & $r_{19} \mid 3\cdot17 \Rightarrow r_{19} = 1, \cancel{3}, \cancel{17}, \cancel{3\cdot17} \Rightarrow$ normal

So let N, Q be the normal Sylow 19, 17-s.g.'s (resp.)

Then NQ is normal of index 3, so now for a Sylow 3-s.g. S, $NQ \cap S = 1$ since orders coprime, so $NQS = G$ and now $G = NQ \rtimes S$.

So have hom: $\varphi: S \longrightarrow Aut(NQ) \cong Aut(\mathbb{Z}_{17} \oplus \mathbb{Z}_{19}) \cong \mathbb{Z}_{16} \oplus \mathbb{Z}_{18}$

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

Now σ_s must be order 1 or 3; if order 1, G abelian, so $G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{17} \oplus \mathbb{Z}_{19}$.

Suppose order 3: $\mathbb{Z}_{16} \oplus \mathbb{Z}_{18} = \langle a \rangle \oplus \langle b \rangle$ has order 3 elts $(1, b^6), (1, b^{12})$, hence only 2 order 3 elts. Now let $\mathbb{Z}_{17} \oplus \mathbb{Z}_{19} \cong \langle \alpha \rangle \oplus \langle \beta \rangle$, and consider $\theta \in Aut(NQ)$ of order 3.

$\theta(\alpha, \beta) = (\alpha, \beta^k)$ so that $k^3 \equiv 1 \pmod{19} \Rightarrow k^3 - 1 \equiv 0 \pmod{19}$

$\Rightarrow (k-1)(k^2+k+1) \equiv 0 \pmod{19} \Rightarrow k^2 + k \equiv 18 \pmod{19} \Rightarrow k(k+1) \equiv 18 \pmod{19}$

$\Rightarrow k = 7$; so $\theta(\alpha, \beta) = (\alpha, \beta^7)$ & $\theta^2(\alpha, \beta) = (\alpha, \beta^{11})$

Therefore let $\sigma_s(\alpha, \beta) = \theta(\alpha, \beta) = (\alpha, \beta^7)$ and hence:

$$G \cong \langle s, \alpha, \beta \mid s^3 = \alpha^{17} = \beta^{19} = 1,\ s\alpha s^{-1} = \alpha,\ s\beta s^{-1} = \beta^7 \rangle$$

② (i) p prime, $q=p^k$, n integer.

Describe condition that guarantees that $\mathbb{F}_q^*$ has an elt order n

Recall that $\mathbb{F}_q^*$ is cyclic, hence it will contain an element of order every divisor of $|\mathbb{F}_q^*| = q-1 = p^k-1$. Hence if $n \mid p^k-1$, then $\exists$ element order n.

(ii) Determine cardinality of $L/\mathbb{F}_3$ splitting field of $x^{13}-1 \in \mathbb{F}_3[x]$ and Structure of $Gal(L/\mathbb{F}_3)$:

We know that $|L| = \mathbb{F}_{3^k}$ for some k. If L is the splitting field of $x^{13}-1$, then it must contain elt order 13, hence $13 \mid |\mathbb{F}_{3^k}^*| = 3^k-1$. If $k=3$ then $3^3-1 = 27-1 = 26 = 2 \cdot 13$, hence $\mathbb{F}_{3^3}$ has an elt order 13, hence $\mathbb{F}_{3^3}$ contains the roots of $x^{13}-1$ (generated as a s.g. of $\mathbb{F}_{3^3}^*$ by the ord 13 elt), hence $\mathbb{F}_{3^3}$ splitting field.

We know that $|Gal(L/\mathbb{F}_3)| = [L:\mathbb{F}_3] = [\mathbb{F}_{3^3}:\mathbb{F}_3] = 3$, hence

$|Gal(L/\mathbb{F}_3)| = 3$, hence $Gal(L/\mathbb{F}_3) \cong \mathbb{Z}_3$ generated by $\sigma(x) = x^p$ (Frob).

---

③ $f(x) = (x^3-2)(x^3-3) \in \mathbb{Q}[x]$, $M \subseteq \mathbb{C}$ splitting field$/\mathbb{Q}$, ω a primitive cube root of unity.

(a) Show $\omega \in M$:

Let $\alpha = \sqrt[3]{2}$ & $\beta = \sqrt[3]{3}$, then $\alpha, \alpha\omega, \alpha\omega^2, \beta, \beta\omega, \beta\omega^2 \in M$.

Then $\alpha^3\omega^3 = 2 \Rightarrow \frac{\alpha^3\omega^2}{2} \cdot \omega = 1$; $\frac{\alpha^3\omega^2}{2} = \frac{\alpha \cdot \alpha \cdot \alpha\omega^2}{2} \in M$,

hence so is its inverse, ω.

(b) Suppose $\beta \notin \mathbb{Q}(\omega,\alpha) \subseteq M$; use this to find $|Gal(M/\mathbb{Q})|$

$$\begin{array}{lcl}
M = \mathbb{Q}(\alpha,\beta,\omega) & & \\
\quad | & 3 & \text{since min poly of } \beta \text{ over } \mathbb{Q}(\omega,\alpha) \text{ is } x^3-3 \\
\mathbb{Q}(\omega,\alpha) & & \\
\quad | & 3 & \text{since min poly of } \alpha \text{ over } \mathbb{Q}(\omega) \text{ is still } x^3-2 \\
\mathbb{Q}(\omega) & & \\
\quad | & 2 & \text{since cyclotomic} \\
\mathbb{Q} & &
\end{array}$$

So by tower law $18 = [M:\mathbb{Q}] = |Gal(M/\mathbb{Q})|$.

(c) How does $Gal(M/\mathbb{Q})$ act on M.

There will be two orbits, each of roots x^3-2 & x^3-3.

(d) Determine $G = Gal(M/\mathbb{Q})$:

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha,\beta,\omega) = M \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha,\omega) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\beta,\omega) \arrow[dl, dash, "3"] \\
 & \mathbb{Q}(\omega) \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Both Galois, hence $Gal(M/\mathbb{Q}(\alpha,\omega)) \trianglelefteq G$
, hence $Gal(M/\mathbb{Q}(\beta,\omega)) \trianglelefteq G$ (*)

both of index 6, so order 3. (& distinct)

By Sylow, $r_3 \equiv 1 \pmod 3$ & $r_3 | 2 \Rightarrow r_3 = 1 \Rightarrow$ Sylow 3-sg. unique.
Both s.g.'s (*) are normal in it and distinct, hence $= \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
(p^2 group hence abelian)

Now, $\mathbb{Q}(\omega)/\mathbb{Q}$ also Galois, so $Gal(M/\mathbb{Q}(\omega)) \trianglelefteq G$ index 2, hence order 3^2

④ In $\mathbb{C}[x,y]$, show $\exists\, m \geq 1$ s.t. $(3x^2+10xy+3y^2)^m \in \underbrace{(x+y-2,\ x^2+y^2-10)}_{= I}$

see that $(x+y-2)^2 = x^2+y^2+2xy-4x-4y+4$
$= x^2+y^2+2xy-4(x+y-1)$

$5(x+y-2)^2 = 5x^2+5y^2+10xy-20(x+y-1)$

$-2(x^2+y^2-10) = -2x^2+-2y^2+20$

so $5(x+y-2)^2 - 2(x^2+y^2-10) = 3x^2+3y^2+10xy+20-20(x+y-1)$
$= 3x^2+3y^2+10xy+-20(x+y-2)$

Hence $3x^2+3y^2+10xy = 5(x+y-2)^2+20(x+y-2)-2(x^2+y^2-10)$,
hence in $I \subseteq \sqrt{I}$.

---

⑤ $g_1, g_2, \ldots, g_m, \ldots \in R$ commutative noeth w/ 1 ; $I \subseteq R$ ideal.
Assume that for each i, $\exists\, k_i \geq 1$ s.t. $g_i^{k_i} \in I$ & show that $\exists\, K$ such that $g_{i_1} \cdots g_{i_K} \in I$ for any choices of g_{i_j}:

Since $\exists\, k_i$ s.t. $g_i^{k_i} \in I$ for each g_i, we have that all $g_i \in \sqrt{I}$.
Now, $\sqrt{I}$ is an ideal of R, which is noetherian, hence $\sqrt{I}$ is finitely generated: $\sqrt{I} = \langle f_1, \ldots, f_\ell \rangle$.

For each f_i, $\exists\, m_i$ s.t. $f_i^{m_i} \in I$, hence let $m = \max\{m_i\}$ and then $f_i^m \in I$ $\forall\, i = 1, \ldots, \ell$.

Now let $g_{i_1}, \ldots, g_{i_K}$ be as above, all in $\sqrt{I}$.

Then $g_{i_j} = \sum_{r=1}^{\ell} a_r^{(j)} f_r$ and $\prod_{j=1}^{K} g_{i_j} = \prod_{j=1}^{K} \left(\sum_{r=1}^{\ell} a_r^{(j)} f_r \right)$

Now let $K = m\ell$; then every term will have total degree $m\ell$ in the f_r's, hence each term must have an $f_r^{\,n}$ term for some r, hence each term is in I, hence the entire sum is in I.

⑥ S finite, $x^5=x\ \forall x\in S$

(i) Show S has no nonzero nilp. els.

Suppose $x^n=0$ ($\exists\, x\neq 0$, n minimal). Clearly $n>5$ since $x^4=0 \Rightarrow x^5=0 \Rightarrow x=0$.

Now let $m=n \pmod 5$ so that $0=x^n=x^{5k}x^m=x^k x^m=x^{k+m}$,

hence contradicting the minimality of n

(ii) Show S is direct sum of $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$

S finite $\Rightarrow$ artinian $\Rightarrow$ $J(S)$ nilpotent $\Rightarrow$ $J(S)=0$ by pt (i).

So S is art + J.S.S. $\Rightarrow$ S.S. $\Rightarrow$ $S\cong M_{n_1}(D_1)\oplus\cdots\oplus M_{n_k}(D_k)$ by A-W.

No nilpotents $\Rightarrow$ $n_i=1\ \forall i$.

Finite $\Rightarrow$ D_i's finite $\Rightarrow$ D_i's fields by little wedd.

$\Rightarrow S\cong F_1\oplus\cdots\oplus F_k$, F_i finite fields, hence $|F_i|=p_i^{e_i}$

Now, we need that $x^5=x$ for all $x\in S$, hence for all $\alpha_i\in F_i$, want $\alpha_i^5=\alpha_i$. Therefore $n\leq 5$ since otherwise els exist w/o this property

Case 1: $F_i=\mathbb{F}_5$; $x^5=x\ \forall x\in F_i$ by def'n.

Case 2: $F_i=\mathbb{F}_2$; $F_i^\times=\{1\}$, hence $1^5=1$ trivially.

Case 3: $F_i=\mathbb{F}_3$; $F_i^\times\cong\mathbb{Z}_2$ $\Rightarrow$ all nonzero $x\in F_i$ have $x^2=1$

$\Rightarrow x^4=1 \Rightarrow x^5=x$,

Case 4: $F_i=\mathbb{F}_4$; $|\mathbb{F}_4^\times|=4-1=3$, hence no elements of order 4 or 2.

(i.e. no els with $x^5=x$), so $F_i\neq\mathbb{F}_4$

So the F_i can be $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$