Algebra Qualifying Exam September 2002

Partial credit is given for partial solutions

1. Let k be a field and let S_n act on the polynomial ring $k[X_1, \ldots, X_n]$ by permuting the variables, i.e. $\sigma \cdot f = f^\sigma$ where

$$f^\sigma(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Show that for any given f, the number of distinct polynomials of the form f^σ is a divisor of $n!$.

2. Show that there are exactly 2 groups of order $11 \cdot 43^2$.

3. Let $f(X) = X^3 - X - 1 \in \mathbb{Q}[X]$. Find the splitting field K of f over $\mathbb{Q}$, the Galois group of the extension $\mathbb{Q} \subseteq K$ and give the number of subfields of K of each degree.

4. Let k be an algebraically closed field, and let $R = k[X_1, \ldots, X_n]$.
a) Show that if $\mathfrak{p}$ is any prime ideal of R, then $\mathfrak{p}$ is an intersection of maximal ideals.
b) If $n = 2$, show that the ideal $\mathfrak{p} = (X_1 + X_2)$ is prime and describe all maximal ideals $\mathfrak{m}$ such that $\mathfrak{p} \subseteq \mathfrak{m}$.

5. Let R be a commutative algebra over the field k, and $A_1, \ldots A_t \in M_n(R)$ be $n \times n$-matrices with entries in R. Show that there exists a k-subalgebra $S \subseteq M_n(R)$ containing A_i, $1 \leq i \leq t$, such that S is (left) noetherian.
(hint: Try to find a subalgebra $R_0 \subseteq R$ such that $S = M_n(R_0)$.)

6. Let R be a finite ring. Show that if $x, y \in R$ satisfy $xy = 1$, then they also satisfy $yx = 1$.
(hint: First consider the case R is semi-simple.)

Algebra - Fall 2002 :

(1) k field, $S_n \curvearrowright k[X_1,\dots,X_n]$ by permuting the variables, i.e. $\sigma \cdot f = f^\sigma$ is given by $f^\sigma(X_1,\dots,X_n) = f(X_{\sigma(1)},\dots,X_{\sigma(n)})$

Show that for any given f, the number of distinct polynomials of the form f^σ is a divisor of $n!$:

Let $f \in k[X_1,\dots,X_n]$. Then under the action, the orbit $\mathcal{O}(f) = \{\sigma \cdot f = f^\sigma : \sigma \in S_n\}$ will include all distinct such f^σ, hence $|\mathcal{O}(f)|$ such f^σ.
Now, letting $G = S_n$, recall that $|\mathcal{O}(f)| = [G : G_f]$, hence by Lagrange, $|\mathcal{O}(f)| \mid |G| = |S_n| = n!$, hence $\mathcal{O}(f) \mid n!$.

(2) Show there are 2 grps $|G| = 11 \cdot 43^2$.

$r_{43} \equiv 1 \pmod{43}$ & $r_{43} \mid 11 \Rightarrow r_{43} = 1$ bc $\not\equiv \Rightarrow N$ sylow 43-sg. normal.

$r_{11} \equiv 1 \pmod{11}$ & $r_{11} \mid 43^2 \Rightarrow r_{11} = 1, 43, 43^2$; let S be 11-sg.

Since $r_{43} = 1$, there are 43^2 elements not order 11, hence $43^2 \cdot 11 - 43^2 = 43^2(11-1) = 43^2 \cdot 10$ elements left. Hence $r_{11} = 43^2$; let S be 11-sg.

Since $N \cap S = 1$, we get $NS = G$, hence $G \cong N \rtimes_\varphi S$, and now we have 2 cases for hom: $\varphi_1 : S \to \mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_{43^2}) \cong \mathbb{Z}_{43(43-1)}$

$\varphi_2 : S \to \mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}_{43} \oplus \mathbb{Z}_{43}) \cong GL_2(\mathbb{F}_{43})$

$|S| = 11$, hence let $S = \langle s \rangle$ and then $\varphi_i(s)$ must be order 1 or 11.

→ continued on attached

(4) Case 1: $\varphi_1: S \to \mathrm{Aut}(N) \cong \mathbb{Z}_{43\cdot 42} \cong \mathbb{Z}_{2\cdot 3\cdot 7\cdot 43} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{43}$.

No order 11 elements, hence only $\varphi_1(s) = 1$, hence abelian: $G \cong \mathbb{Z}_{11} \oplus \mathbb{Z}_{43}^2$

Case 2: $\varphi_2: S \to \mathrm{Aut}(N) \cong GL_2(\mathbb{F}_{43})$.

order 1 $\Rightarrow$ $G \cong \mathbb{Z}_{11} \oplus \mathbb{Z}_{43} \oplus \mathbb{Z}_{43}$, so look for $a \in GL_2(\mathbb{F}_{43})$ s.t. $a^{11} = 1$.

Note that $|GL_2(\mathbb{F}_{43})| = (43^2-1)(43)(43-1) = 2^3 \cdot 3^2 \cdot 7^2 \cdot 11 \cdot 43$, hence the Sylow 11-sg. is cyclic, hence any order 11 elt. is conjugate to another, hence all in same similarity class and induce same relation, giving us third group.

$|GL_2(\mathbb{F}_{43})| =$

$$(43^2-1)(43^2-43) = (43^2-1)(43)(43-1)$$
$$= (43-1)^2(43+1)43$$
$$= 42^2 \cdot 44 \cdot 43 = 2\cdot 11 \cdot 2^2 \cdot 3^2 \cdot 7^2 \cdot 43$$
$$= 2^3 3^2 7^2 \cdot 11 \cdot 43$$

(3) $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$; Find splitting field, Galois group, & subfields.

First, see that $f(1) = -1$ and $f(2) = 8 - 2 - 1 = 5$, hence by the IVT, $\exists \alpha \in (1,2)$ such that $f(\alpha) = 0$, hence f has at least one real root, and f has a factor of $(x - \alpha)$. Now:

$$(x-\alpha) \overline{)\, x^3 - x - 1 \;\big|\; x^2 + \alpha x + (\alpha^2 - 1)}$$

$x^3 - \alpha x^2$

$\alpha x^2 - x - 1$

$\alpha x^2 - \alpha^2 x$

$(\alpha^2 - 1)x - 1$

$(\alpha^2 - 1)x - \alpha(\alpha^2 - 1)$

$\alpha(\alpha^2 - 1) - 1 \Rightarrow \boxed{\alpha(\alpha^2 - 1) = 1}$

- Now $f(x) = (x - \alpha)(x^2 + \alpha x + (\alpha^2 - 1))$ & $\alpha(\alpha^2 - 1) = 1$, and now the other two roots are $\beta, \bar{\beta} = \dfrac{-\alpha \pm \sqrt{\alpha^2 - 4(\alpha^2 - 1)}}{2}$

Suppose that both are real, hence $\alpha^2 \geq 4(\alpha^2 - 1) \Rightarrow 3\alpha^2 \leq 4$

$\Rightarrow \alpha^2 \leq \frac{4}{3} \Rightarrow \alpha \leq \sqrt{\frac{4}{3}} = \frac{2}{\sqrt{3}}$, hence $\alpha \in (1, \frac{2}{\sqrt{3}})$ (*)

- Consider $f'(x) = 3x^2 - 1$; clearly $f'(x) > 0$ for all $x \in (1,2)$, hence f is nondecreasing over $(1,2)$, hence $f(x)$ will only change signs once over $(1,2)$, hence α is the unique root in $(1,2)$; but, $f(\frac{2}{\sqrt{3}}) = (\frac{2}{\sqrt{3}})^3 - (\frac{2}{\sqrt{3}}) - 1 = \frac{8}{3\sqrt{3}} - \frac{6}{3\sqrt{3}} - \frac{3\sqrt{3}}{3\sqrt{3}}$

$= \dfrac{2 - 3\sqrt{3}}{3\sqrt{3}} < 0$, hence f is negative from $(1, \frac{2}{\sqrt{3}})$, hence there is no root in this interval, hence contradiction to (*).

Therefore β and $\bar{\beta}$ are a complex conjugate pair;

recall $\beta = \dfrac{-\alpha + \sqrt{4 - 3\alpha^2}}{2}$, hence $\mathbb{Q}(\alpha, \beta, \bar{\beta}) = \mathbb{Q}(\alpha, \beta) \supsetneq \mathbb{Q}(\alpha)$.

Clearly $L = \mathbb{Q}(\alpha, \beta, \bar{\beta}) = \mathbb{Q}(\alpha, \beta)$ is the splitting field

See then: $L = \mathbb{Q}(\alpha,\beta)$, $\mathbb{Q}(\alpha)$, $\mathbb{Q}$

② since β has min polynomial $x^2 + \alpha x + (\alpha^2 - 1)$ over $\mathbb{Q}(\alpha)$.

③ since deg min poly of $\alpha \leq 3$ (since $f(\alpha) = 0$ & $\deg f \leq 3$) & $3 \mid [L:\mathbb{Q}]$

$3 = \deg f \mid [L:\mathbb{Q}]$.

Therefore $[L:\mathbb{Q}] = 6$ by towers law.

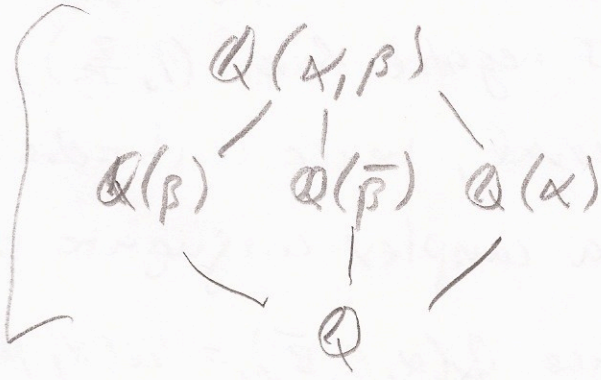
Now, since $\beta \notin \mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois, hence $\mathrm{Gal}(E/\mathbb{Q}(\alpha)) \leq \mathrm{Gal}(E/\mathbb{Q})$ is not a normal subgroup. However, every s.g. of an abelian grp is normal, hence $\mathrm{Gal}(E/\mathbb{Q})$ is nonabelian, hence

$\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$

Recall $\beta = \frac{-\alpha + \sqrt{4-3\alpha^2}}{2}$ & $\overline{\beta} = \frac{-\alpha - \sqrt{4-3\alpha^2}}{2}$; then $\beta + \overline{\beta} = -\alpha$

Suppose that $\overline{\beta} \in \mathbb{Q}(\beta)$; then $-\alpha = \beta + \overline{\beta} \in \mathbb{Q}(\beta)$, hence $\alpha \in \mathbb{Q}(\beta)$, hence $L = \mathbb{Q}(\beta)$, hence $[L:\mathbb{Q}] \leq 3$, a contradiction.

Hence $\overline{\beta} \notin \mathbb{Q}(\beta)$ and then subfields are:



④ k algebraically closed, $R = k[X_1, \dots, X_n]$.

(a) Show a prime ideal $P \subseteq R$ is the intersection of maximal ideals.

Let $P \subseteq R$ be prime ideal. Then P is a radical ideal, hence $P = \sqrt{P}$, and then: $P = \sqrt{P} = Id(Var(P)) = Id\left(\bigcup_{i \in I} \{\alpha_i\}\right)$

$$= \bigcap_{i \in I} (\alpha_i - X)$$

where $\alpha_i = (\alpha_i^1, \dots, \alpha_i^n)$ & $X = (X_1, \dots, X_n)$

Since k algebraically closed, $(\alpha_i - X)$ are maximal ideals, hence P is intersection of max ideals.

(b) For $n = 2$, show that $P = (X_1 + X_2)$ is prime & describe all max ideals M s.t. $P \subseteq M$.

The maximal ideals of $k[X_1, X_2]$ have the form $(X_1 - \alpha_1, X_2 - \alpha_2)$ since k is algebraically closed. So then if $(X_1 + X_2) \subseteq (X_1 - \alpha_1, X_2 - \alpha_2)$, we would have $X_1 + X_2 = (X_1 - \alpha_1) + (X_2 - \alpha_2) \Rightarrow \alpha_1 = -\alpha_2$, hence the max ideals containing $(X_1 + X_2)$ are of form $(X_1 - a, X_2 + a)$ for all $a \in k$.

Clearly $(X_1 + X_2)$ is prime since $X_1 + X_2$ is irreducible in $k[X_1, X_2]$.

(OR see that $k[X, Y]/(X+Y) \cong k[X]$, hence int. domain, hence $(X+Y)$ prime)

Also may use generalized Eisenstein

⑤ R commutative k-algebra (k field), $A_1, \dots, A_t \in M_n(R)$.
Show that $\exists$ k-subalg $S \subseteq M_n(R)$ containing $A_i \; \forall i$ s.t. S is noetherian.

- R k-alg, hence $M_n(R)$ k-alg as well.
- Recall that a fin-gen k-algebra R over noetherian ring k is itself noetherian: let $\{r_1, \dots, r_n\}$ be generating set of R. Then $\exists$ surj. hom
$$f: k[X_1, \dots, X_n] \twoheadrightarrow R \quad ; \quad k \text{ noeth} \Rightarrow k[X_1, \dots, X_n] \text{ noeth (Hilbert)}$$
$$\Rightarrow R = f(k[X_1, \dots, X_n]) \text{ noeth.}$$
since f homomorphism
(*)
- Now, see that $\{$entries of A_i's$\} \subseteq R$, and let $R_0 = \langle$entries of A_i's$\rangle$ be a k-algebra. Then $M_n(R_0) \subseteq M_n(R)$ is a k-subalgebra; now we'll show $M_n(R_0)$ is fin-gen as k-algebra.
- Consider the set $B = \left\{ M_{ijl} = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & r & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 1 & \cdots & 0 \end{pmatrix} \right.$ (r in ith row, jth column) $\Big| \; i,j = 1, \dots, n, \; l = 1, \dots, t, \; r$ the ij^{th} entry of $A_l \Big\}$

Each A_l has n^2 entries, hence $|B| = tn^2 < \infty$, and clearly B generates $M_n(R_0)$, hence $M_n(R_0)$ is finitely-generated k-alg; but k field, hence noeth, hence by (*), $M_n(R_0)$ is noetherian, and it contains each of $A_1, \dots, A_t$; so let $S = M_n(R_0)$.

⑥ R finite ring; show if $x, y \in R$ have $xy = 1$, then $yx = 1$.

R finite $\Rightarrow$ R noetherian; suppose $x, y \in R$ s.t. $xy = 1$ & define $\varphi: R \to R$ a $\mapsto ya$.
This map is surjective since $\varphi(x) = xy = 1$; now consider the following chain: $\ker\varphi \subseteq \ker\varphi^2 \subseteq \cdots \subseteq \ker\varphi^n = \ker\varphi^{n+1}$; let $r \in \ker\varphi$.
Then since φ surjective $\Rightarrow \varphi^n$ surjective, $\exists\, s \in R$ s.t. $r = \varphi^n(s) \Rightarrow 0 = \varphi(r) = \varphi^{n+1}(s)$
$\Rightarrow s \in \ker\varphi^{n+1} = \ker\varphi^n \Rightarrow 0 = \varphi^n(s) = r \Rightarrow r = 0$; hence $\ker\varphi = 0$

[OR: since R finite, φ surjective $\Leftrightarrow$ φ injective $\Leftrightarrow \ker\varphi = 0$]

Now see that $\varphi(1 - yx) = (1 - yx)y = y - yxy = y - y(1) = 0$
$\Rightarrow 1 - yx \in \ker\varphi \Rightarrow 1 - yx = 0 \Rightarrow \underline{1 = yx}$.