RETURN THIS COVER SHEET WITH YOUR EXAM AND SOLUTIONS!

Algebra
Ph.D. Preliminary Exam

August 18, 2008

INSTRUCTIONS:

1. Answer each question on a separate page. Turn in a page for each problem even if you cannot do the problem.

2. Label each answer sheet with the problem number.

3. Put your number, not your name, in the upper right hand corner of each page. If you have not received a number, please choose one (1234 for instance) and notify the graduate secretary as to which number you have chosen.

4. There are 6 problems, each worth 17 points. The numbers of points for each problem and section thereof is listed beside it.

Algebra Prelim **August 2008**

1) (17 pts) Show that a group G of order $2^3 \cdot 5 \cdot 13$ cannot be simple.

2) (17 pts) Let G be a finite group which acts on a set S on both the left and the right. For an element $s \in S$, let Gs and sG denote the orbit of s under these respective actions.

These actions can be combined into a single (left) action of $G \times G$ on S via $(g,h)s = gsh^{-1}$. The corresponding orbit of s under this action is denoted GsG. There are two independent questions one wants to answer about such orbits: what is their size, and how many of them are there?

a) (12 pts) For $s \in S$, show that the size of GsG,

$$|GsG| = \frac{|sG||Gs|}{|Gs \cap sG|}.$$

b) (5 pts) Show that the number of such orbits GsG in S is

$$\frac{1}{|G|^2} \sum_{g,h \in G} |\{s \in S \mid gsh^{-1} = s\}|.$$

3. Let p be a prime number in the ring of integers $\mathbb{Z}$. Let A be the set

$$\left\{\frac{a}{b} \in \mathbb{Q} : a,\ b \in \mathbb{Z},\ p \not| \, b\right\},$$

where $\mathbb{Q}$ is the field of rational numbers.

a) (3 pts) Show that A is a subring of $\mathbb{Q}$, and is an integral domain.

b) (7 pts) Show that for every non-zero $\alpha \in A$, there is a unique unit $u \in A$ and a unique non-negative integer e, such that $\alpha = up^e$.

c) (7 pts) Show that A is a Euclidean domain.

4. (17 pts) Let $R = M_2(\mathbb{Q})$ denote the ring of 2×2 matrices with entries in the rational field $\mathbb{Q}$, and $I \in R$ denote the identity matrix.

a) (9 pts) Show that all $A \in R$, $A \neq I$, that satisfy $A^3 = I$, are similar (via a matrix in R) to each other.

b) (8 pts) Let n be any odd positive integer. Show that there is no $A \in R$ for which (i) $A \neq I$, (ii) $A^n = I$, and (iii) 1 is an eigenvalue of A.

5) (17 pts) Let k be a field, and $f \in k[x]$ an irreducible polynomial. Let α be a root of f in a splitting field of f over k. Suppose that $\alpha + 1$ is also a root of f.

a) (8 pts) Show that k has characteristic p for some prime number p.

b) (9 pts) Let $\beta = \alpha^p - \alpha$. Show that the degree of $k(\alpha)$ over $k(\beta)$ is p.

6) (17 pts) Let K be the splitting field of $f = x^4 + 2x^2 - 2$ over the field of rational numbers $\mathbb{Q}$. Determine the Galois group G of K over $\mathbb{Q}$.

Solutions

1) Suppose G has this order (520) and is not simple. Then the number r of 13-sylow subgroups is congruent to 1 mod 13 and divides $2^3 \cdot 5$, so $r = 40$. Hence G has $40 \cdot 12 = 480$ elements of order 13. The same argument shows it has $s = 26$, 5-sylow subgroups, so $26 \cdot 4 = 104$ elements of order 5. But $480 + 104 > 520$, a contradiction.

2) a) Let G/S be the space of orbits of S under the left action of G on S. Then the action on the right of G on S induces an action r of G on G/S. For some $s \in S$, GsG is the union of the elements in the orbit of Gs under r. Each element in this orbit has the same cardinality, so

$$|GsG| = |Gs|(|G|/|T|),$$

where T is the stabilizer of Gs in G under r. Now T acts on the elements of Gs, and has a subgroup U which stabilizes s, which is also the stabilizer of s in the right action of G on S. So $|T|/|U|$ is the size of the orbit of s under T, which is $|Gs \cap sG|$. Hence

$$|GsG| = |Gs|(|G|/|U||Gs \cap sG|) = |Gs||sG|/|Gs \cap sG|.$$

b) The hint does it, along with the orbit counting theorem (Burnside's Lemma): for a group H acting on a set T, the number of orbits is

$$\frac{1}{|H|} \sum_{h \in H} \#\{t \in T | ht = t\}.$$

3. a) Note $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$, and that p being prime means $p \not| bd$ if $p \not| b$ and $p \not| d$. Then A is an integral domain, since $A \subset \mathbb{Q}$.

b) Let $x \neq 0$ in A. Clearly, $x = \frac{a}{b}p^k$, where $a, b \in \mathbb{Z}, p \not| a, p \not| b$, and $k = 0, 1, 2, ...$ Since $p \not| a$, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in A$, hence $u := \frac{a}{b} \in A^\times$. Now suppose that $x = \frac{a}{b}p^k = \frac{c}{d}p^l$, where $a, b, c, d \in \mathbb{Z}$ are not divisible by p, and $k, l \in \{0, 1, 2, ...\}$. Then $adp^k = bcp^l \in \mathbb{Z}$. Since p does not divide a, b, c, or d, and $\mathbb{Z}$ is a UFD, it is immediate that $k = l$ and that $\frac{a}{b} = \frac{c}{d}$. With this it makes sense to define $\rho(ux^e) = e$.

c) Let $x = up^e$ and $y = vp^f$ be elements of $A - \{0\}$, where $u, v \in A^\times$, and $e, f \in \{0, 1, 2, ...\}$. Then we see that $x = y \cdot \frac{u}{v}p^{e-f} + 0$ if $e \geq f$; and that $x = y \cdot 0 + x$ if $e < f$. In the first case, recall that u and $v \in A^\times$, and that $\frac{u}{v}p^{e-f} \in A$, and we see that the remainder is 0. In the second case, note $\rho(x) = e < f = \rho(y)$. This shows that ρ makes A a Euclidean domain.

4. a) Let B be the rational canonical form of A, so also $B^3 = I$. If B is diagonal, then $B = I$, so $A = I$, a contradiction. So

$$B = \begin{pmatrix} 0 & 1 \\ -d & t \end{pmatrix}$$

where d and t are respectively the determinant and trace of A. Since $d^3 = 1$ and $d \in \mathbb{Q}$, $d = 1$. One can now calculate B^3 and see it is I precisely when $t = -1$. More elegantly, the eigenvalues of A are cuberoots of unity, and the only way 2 of them add to a rational number is that the sum of the complex ones are -1, and the sum of 1 and 1 is 2. But in the latter case, the Jordan canonical form would have to be I (a contradiction of $A \neq I$), or

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which is not of order 3. So $t = -1$. Since all such A have the same rational canonical form, they all are similar (over $\mathbb{Q}$) to each other.

b) As in (a), $d = 1$, so if A has an eigenvalue of 1, both roots of its characteristic polynomial must be 1. Hence if $A \neq I$, then its Jordan canonical form B must be

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

so B^n cannot be I.

5) a) Solution 1: (Without galois theory) We can assume without loss of generality that f is monic, so $f(x)$ is the minimal polynomial of α over k. But by assumption, α is also a root of $f(x+1)$, so $f(x)|f(x+1)$, hence $f(x) = f(x+1)$ since they are both monic of the same degree. Therefore $\alpha + 1$ is a root of $f(x+1)$, so $\alpha + 2$ is a root of $f(x)$. By induction, $\alpha + n$ is a root of $f(x)$ for any positive integer n. Since f only has only finitely many roots, the set $\alpha + n$, $n \geq 0$ is a finite set. Hence k is not characteristic 0, so must be of characteristic p for some prime p.

Solution 2: Since α and $\alpha + 1$ are roots of the irreducible polynomial f, there is a field isomorphism ϕ mapping $k(\alpha)$ to $k(\alpha+1)$, fixing k, with $\phi(\alpha) = \alpha+1$. Since $k(\alpha) = k(\alpha+1)$, ϕ is a field automorphism of $k(\alpha)$ over k. By induction, for any positive n, $\phi^n(\alpha) = \alpha + n$. Now $k(\alpha)/k$ is a finite algebraic extension, so its galois group G is finite, so ϕ^m is the identity for some m. Hence $m = 0$ in k, and k is of characteristic p for some p.

b) Since α is a root of $x^p - x = \beta$ over $k(\beta)$, the degree of $k(\alpha)$ over $k(\beta)$ is at most p. Conversely, letting ϕ be as in (a) (Solution 2), β is fixed by ϕ, hence by the subgroup generated by ϕ, which is of order p. Hence if L is the fixed field of $k(\alpha)$ by the subroup generated by ϕ, then $[k(\alpha) : L] = p$, and L contains $k(\beta)$. Hence $L = k(\beta)$ and we are done.

6) By Eisenstein's criterion, f is irreducible over $\mathbb{Z}$, and by Gauss's Lemma, it's irreducible over $\mathbb{Q}$. So if α is a root of f in K, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Note that $-\alpha$ is another root of f in K: let β be another. Than $-\beta$ is the fourth, so $K = \mathbb{Q}(\alpha, \beta)$, and $[K : \mathbb{Q}(\alpha)] = 1$ or 2. To determine which, let us embed K into the complex numbers. Then α^2 and β^2 are the roots of $x^2 + 2x - 2$, so by the quadratic formula are $-1 \pm \sqrt{3}$, which are real. Let α and β be such that $\alpha^2 = -1 + \sqrt{3} > 0$, so α is real. Then $\beta^2 = -1 - \sqrt{3} < 0$, so β is not real. Hence $\beta \notin \mathbb{Q}(\alpha)$, and $[K : \mathbb{Q}] = 8$. Since f is irreducible, its galois group

can be realized as a subgroup of S_4, so since its order 8, it is a 2-sylow subgroup of S_4. Hence G is the dihedral group D_4. Alternatively, since $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$, then $\mathbb{Q}(\alpha)$ is not a normal extension of $\mathbb{Q}$, so G must be a non-abelian group of order 8. Furthermore, the same fact shows that $K/\mathbb{Q}(\sqrt{3})$ is a galois extension of degree 4 which has more than one quadratic intermediate extension, so has a galois group which is the Klein 4-group. Since the quaternion group has no normal subgroups of this type, G must be D_4.