Algebra Prelim

June 2004

Provide proofs for all statements, citing any theorems that may be needed.
If necessary, you may use the results from other parts of this test, even though you may not have successfully proved them.

1. Let K be the splitting field of the polynomial $X^8 - 1$ over $\mathbb{Q}$.

   (a) What is the field degree $[K : \mathbb{Q}]$?

   (b) Describe the Galois group $\mathrm{G}(K, \mathbb{Q})$ completely.

---

2. Let G be a finite group and let H be a subgroup of index n, i.e. $[G : H] = n$. Let C be the n left cosets of H in G and let S_n denote the group of permutations of the set C.

   For $g \in G$ let $\tau(g)$ be the map from C to C defined by $\tau(g)(aH) = gaH$ for any $aH \in C$.

   (a) Argue that the map $\tau(g)$ is a permutation of C and thus we get a map $\tau : G \longrightarrow S_n$ which maps $g \in G$ to $\tau(g) \in S_n$.

   (b) Show that τ is a group homomorphism.

   (c) Argue that $Ker(\tau) \subset H$.

   (d) Prove that
   $$Ker(\tau) = \bigcap_{a \in G} aHa^{-1}.$$

---

3. Let
   $$S = \{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \}.$$

   (a) Prove that S is a subring of the usual ring of 2 by 2 real matrices $M_{2\times 2}(\mathbb{R})$.

   (b) Prove that S is isomorphic to the field $\mathbb{C}$ of complex numbers.

---

4. Up to isomorphisms, describe all the homomorphic images of the ring
   $$\mathbb{Q}[X]/((X-2)^2(X-3)).$$

Please turn over $\cdots$

Continued from the other side $\cdots$

5. Let K a field and let K^* be the set of units in K.

   For all $a \in K^*$ and $b \in K$ define a function $f_{a,b} : K \longrightarrow K$ by

   $$f_{a,b}(\alpha) = a\alpha + b \qquad \forall \alpha \in K.$$

   Let $\qquad A(K) = \{f_{a,b} \mid a \in K^* \text{ and } b \in K\}.$

   (a) Show that each $f_{a,b} \in A(K)$ is a bijection.

   (b) Show that $A(K)$ is closed under composition.

   (c) Further show that $A(K)$ is a group under composition.

   (d) Show that $H = \{f_{1,b} | b \in K\}$ is a normal subgroup of $A(K)$.

   (e) Argue that $A(K)$ is isomorphic to the group of K-automorphisms of the polynomial ring $K[X]$.

   (Recall that a K-automorphism of $K[X]$ is an automorphism of $K[X]$ which restricts to the identity on K.)

---

6. Let $f \in \mathbb{Q}[X, Y]$, the polynomial ring in two variables over the rational numbers, and suppose that

   $$f = f(X, Y) = Y^n + \sum_{i=0}^{i=n-1} a_i(X)Y^i \text{ where } a_i(X) \in \mathbb{Q}[X] \text{ for } 0 \leq i \leq (n-1).$$

   (a) Suppose that f is irreducible modulo X, i.e. $f(0, Y)$ is irreducible in $\mathbb{Q}[Y]$. Argue that f must be irreducible in $\mathbb{Q}[X, Y]$.

   (b) Using the above or otherwise, prove that $Y^5 + 2Y^2 + 3X^4Y + X^7 + 6$ is irreducible in $\mathbb{Q}[X, Y]$. Justify all your claims.

---

7. Let p be a prime number **different from** 5 and 7. Let L be the splitting field of $X^{35} - 1$ over F_p, the Galois field with p elements.

   (a) Argue that L is a separable extension of F_p.

   (b) Show that $[L : F_p]$ is the smallest integer m such that p^m is congruent to 1 modulo 35. Explain all reasoning.
