**Algebra Prelim**
**September 12, 2011**

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let $\mathrm{GL}_2(\mathbb{C})$ be the general linear group of $2\times 2$ complex matrices, let H be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ consisting of non-zero multiples of the identity matrix, and let $\mathrm{PGL}_2(\mathbb{C})$ be the quotient group $\mathrm{GL}_2(\mathbb{C})/\,\mathrm{H}$.

   Let $A, B \in \mathrm{PGL}_2(\mathbb{C})$, and assume that both elements have order $n$. Prove that there exist $C \in \mathrm{PGL}_2(\mathbb{C})$ and a positive integer $m$ such that

   $$CBC^{-1} = A^m.$$

2. In this problem, as you apply Sylow's Theorem, state precisely which portions you are using.

   (a) Prove that there is no simple group of order 30.

   (b) Suppose that $G$ is a simple group of order 60. Determine the number of $p$-Sylow subgroups of $G$ for each prime $p$ dividing 60, then prove that $G$ is isomorphic to the alternating group $A_5$.

   Note: In the second part, you needn't show that $A_5$ is simple. You need only show that if there is a simple group of order 60, then it must be isomorphic to $A_5$.

3. Describe the Galois group and the intermediate fields of the cyclotomic extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

4. Let

   $$R = \mathbb{Z}[x]/(x^2 + x + 1).$$

   (a) Answer the following questions with suitable justification.

   i. Is $R$ a Noetherian ring?

   ii. Is $R$ an Artinian ring?

   (b) Prove that $R$ is an integrally closed domain.

5. Let $R$ be a commutative ring. Recall that an element $r$ of $R$ is *nilpotent* if $r^n = 0$ for some positive integer $n$ and that the *nilradical* of $R$ is the set $N(R)$ of nilpotent elements.

   (a) Prove that
   $$N(R) = \bigcap_{P \text{ prime}} P.$$
   (Hint: Given a non-nilpotent element $r$ of $R$, you may wish to construct a prime ideal that does not contain $r$ or its powers.)

   (b) Given a positive integer $m$, determine the nilradical of $\mathbb{Z}/(m)$.

   (c) Determine the nilradical of $\mathbb{C}[x,y]/(y^2 - x^3)$.

   (d) Let $p(x,y)$ be a polynomial in $\mathbb{C}[x,y]$ such that for any complex number $a$, $p(a, a^{3/2}) = 0$. Prove that $p(x,y)$ is divisible by $y^2 - x^3$.

6. Given a finite group $G$, recall that its *regular representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by left multiplication of $G$ on itself and its *adjoint representation* is the representation on the complex group algebra $\mathbb{C}[G]$ induced by conjugation of $G$ on itself.

   (a) Let $G = \mathrm{GL}_2(\mathbb{F}_2)$. Describe the number and dimensions of the irreducible representations of $G$. Then describe the decomposition of its regular representation as a direct sum of irreducible representations.

   (b) Let $H$ be a group of order 12. Show that its adjoint representation is reducible; that is, there is an $H$-invariant subspace of $\mathbb{C}[H]$ besides 0 and $\mathbb{C}[H]$.

7. Let $M$, $N$ be finitely generated modules over $\mathbb{Z}$. Recall that $\mathrm{Ann}(M)$ is the ideal in $\mathbb{Z}$ defined as follows:
   $$\mathrm{Ann}(M) = \{a \in \mathbb{Z} \mid am = 0 \text{ for any } m \in M\}$$
   Prove that $M \otimes_{\mathbb{Z}} N = 0$ if and only if $\mathrm{Ann}(M) + \mathrm{Ann}(N) = (1)$.

8. Let $R$ be a commutative integral domain. Show that the following are equivalent:

   (a) $R$ is a field;

   (b) $R$ is a semi-simple ring;

   (c) Any $R$-module is projective.

# 2010 Algebra Prelim

August 31, 2010

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count for more than several partial solutions. Always justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. Let $p$ be a positive prime number, $\mathbb{F}_p$ the field with $p$ elements, and let $G = \mathrm{GL}_2(\mathbb{F}_p)$.

   (a) Compute the order of $G$, $|G|$.

   (b) Write down an explicit isomorphism from $\mathbb{Z}/p\mathbb{Z}$ to

   $$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{F}_p \right\}.$$

   (c) How many subgroups of order $p$ does $G$ have?
   **Hint:** compute $gug^{-1}$ for $g \in G$ and $u \in U$; use this to find the size of the normalizer of $U$ in $G$.

2. (a) Give definitions of the following terms: (i) a finite length (left) module, (ii) a composition series for a module, and (iii) the length of a module,

   (b) Let $l(M)$ denote the length of a module $M$. Prove that if

   $$0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$$

   is an exact sequence of modules of finite length, then

   $$\sum_{i=1}^{n} (-1)^i l(M_i) = 0.$$

3. Let $\mathbb{F}$ be a field of characteristic $p$, and $G$ a group of order $p^n$. Let $R = \mathbb{F}[G]$ be the group ring (group algebra) of $G$ over $\mathbb{F}$, and let $u := \sum_{x \in G} x$ (so $u$ is an element of $R$).

   (a) Prove that $u$ lies in the center of $R$.

(b) Verify that $Ru$ is a 2-sided ideal of $R$.

(c) Show there exists a positive integer $k$ such that $u^k = 0$. Conclude that for such a $k$, $(Ru)^k = 0$.

(d) Show that $R$ is **not** a semi-simple ring. (**Warning:** Please use the definition of a semisimple ring; do **not** use the result that a finite length ring fails to be semisimple if and only if it has a non-zero nilpotent ideal.)

4. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (where $a_n \neq 0$) and let $R = \mathbb{Z}[x]/(f)$. Prove that $R$ is a finitely-generated module over $\mathbb{Z}$ if and only if $a_n = \pm 1$.

5. Consider the ring

$$S = C[0,1] = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$$

with the usual operations of addition and multiplication of functions.

(a) What are the invertible elements of $S$?

(b) For $a \in [0,1]$, define $I_a = \{f \in S \mid f(a) = 0\}$. Show that $I_a$ is a maximal ideal of $S$.

(c) Show that the elements of any proper ideal of $S$ have a common zero, i.e., if $I$ is a proper ideal of $S$, then there exists $a \in [0,1]$ such that $f(a) = 0$ for all $f \in I$. Conclude that every maximal ideal of $S$ is of the form $I_a$ for some $a \in [0,1]$.
**Hint:** as $[0,1]$ is compact, every open cover of $[0,1]$ contains a finite subcover.

6. (a) Let $L/F$ be a field extension that is finite and Galois. Show that if the Galois group $\mathrm{Gal}(L/F)$ is abelian then for every intermediate field $F \subseteq K \subseteq L$, $K/F$ is also a Galois extension.

(b) Let $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right) \subset \mathbb{R}$. Show that $K/\mathbb{Q}$ is an extension of degree 4 that is **not** Galois.

(c) Let $L$ be the smallest Galois extension of $\mathbb{Q}$ that contains $K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$. Compute the group $\mathrm{Gal}(L/\mathbb{Q})$.

7. Let $F$ be a field of characteristic zero, and let $K$ be an **algebraic** extension of $F$ that possesses the following property: every polynomial $f \in F[x]$ has a root in $K$. Show that $K$ is algebraically closed.
**Hint:** if $K(\theta)/K$ is algebraic, consider $F(\theta)/F$ and its normal closure; primitive elements might be of help.

8. Let $G$ be the unique non-abelian group of order 21.

(a) Describe all 1-dimensional complex representations of $G$.

(b) How many (non-isomorphic) irreducible complex representations does $G$ have and what are their dimensions?

(c) Determine the character table of $G$.

## Algebra Preliminary Exam — September 14, 2009

**Instructions:** Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

1. (a) Classify groups of order $2009 = 7^2 \times 41$.
   (b) Suppose that $F$ is a field and $K/F$ is a Galois extension of degree 2009. How many intermediate fields are there – that is, how many fields $L$ are there with $F \subset L \subset K$, both inclusions proper? (There may be several cases to consider.)

2. Let $K$ be a field. A discrete valuation on $K$ is a function $\nu : K\backslash\{0\} \to \mathbb{Z}$ such that

   (i) $\nu(ab) = \nu(a) + \nu(b)$
   (ii) $\nu$ is surjective
   (iii) $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}\ \forall\ a, b \in K\backslash\{0\}$ with $a + b \neq 0$

   Let $R := \{x \in K\backslash\{0\} : \nu(x) \geq 0\} \cup \{0\}$. Then $R$ is called the valuation ring of $\nu$.

   Prove the following:

   (a) $R$ is a subring of $K$ containing the 1 in $K$.
   (b) for all $x \in K\backslash\{0\}$, either $x$ or $x^{-1}$ is in $R$.
   (c) $x$ is a unit of $R$ if and only if $\nu(x) = 0$.
   (d) Let $p$ be a prime number, $K = \mathbb{Q}$ and $\nu_p : \mathbb{Q}\backslash\{0\} \to \mathbb{Z}$ be the function defined by $\nu_p(\frac{a}{b}) = n$ where $\frac{a}{b} = p^n \frac{c}{d}$ and $p$ does not divide $c$ and $d$. Prove that the corresponding valuation ring $R$ is the ring of all rational numbers whose denominators are relatively prime to $p$.

3. Let $F$ be a field of characteristic not equal to 2.

   (a) Prove that any extension $K$ of $F$ of degree 2 is of the form $F(\sqrt{D})$ where $D \in F$ is not a square in $F$ and conversely, that each such extension has degree 2 over $F$.
   (b) Let $D_1, D_2 \in F$ neither of which is a square in $F$. Prove that $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$ if $D_1 D_2$ is not a square in $F$ and is of degree 2 otherwise.

4. Let $F$ be a field and $p(x) \in F[x]$ an irreducible polynomial.

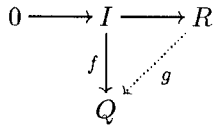
   (a) Prove that there exists a field extension $K$ of $F$ in which $p(x)$ has a root.

   (b) Determine the dimension of $K$ as a vector space over $F$ and exhibit a vector space basis for $K$.

   (c) If $\theta \in K$ denotes a root of $p(x)$, express $\theta^{-1}$ in terms of the basis found in part (b).

   (d) Suppose $p(x) = x^3 + 9x + 6$. Show $p(x)$ is irreducible over $\mathbb{Q}$. If $\theta$ is a root of $p(x)$, compute the inverse of $(1 + \theta)$ in $\mathbb{Q}(\theta)$.

5. Let $R$ be a ring and $Q$ an $R$-module. According to Baer's criterion, $Q$ is injective if and only if for every ideal $I$ of $R$, any $R$-module map $f : I \to Q$ may be extended to an $R$-module map $g : R \to Q$:




   (a) Suppose that $p$ is prime and $n$ is a positive integer with $p$ dividing $n$. Then multiplication makes $\mathbb{Z}/p\mathbb{Z}$ into a module over the ring $\mathbb{Z}/n\mathbb{Z}$. Show that $\mathbb{Z}/p\mathbb{Z}$ is injective as a $\mathbb{Z}/n\mathbb{Z}$-module if and only if $p^2$ does not divide $n$.

   (b) Prove that if $R$ is a PID, then an $R$-module $Q$ is injective if and only if $rQ = Q$ for every nonzero $r \in R$.

6. Fix a ring $R$, an $R$-module $M$, and an $R$-module homomorphism $f : M \to M$.

   (a) If $M$ satisfies the descending chain condition on submodules, show that if $f$ is injective, then $f$ is surjective. (Hint: note that if $f$ is injective, so are $f \circ f$, $f \circ f \circ f$, etc.)

   (b) Give an example of a ring $R$, an $R$-module $M$, and an injective $R$-module homomorphism $f : M \to M$ which is not surjective.

   (c) If $M$ satisfies the ascending chain condition on submodules, show that if $f$ is surjective, then $f$ is injective.

   (d) Give an example of a ring $R$, an $R$-module $M$, and a surjective $R$-module homomorphism $f : M \to M$ which is not injective.

7. Let $G$ be a finite group, $k$ an algebraically closed field, and $V$ an irreducible $k$-linear representation of $G$.

(a) Show that $\mathrm{Hom}_{kG}(V,V)$ is a division algebra with $k$ in its center.

(b) Show that $V$ is finite-dimensional over $k$, and conclude that $\mathrm{Hom}_{kG}(V,V)$ is also finite-dimensional.

(c) Show the inclusion $k \to \mathrm{Hom}_{kG}(V,V)$ found in (a) is an isomorphism. (For $f \in \mathrm{Hom}_{kG}(V,V)$, view $f$ as a linear transformation and consider $f - \alpha I$, where $\alpha$ is an eigenvalue of $f$.)

8. Recall the following basic definitions and facts about ideals and varieties. Let $k$ be a field and $n$ be a positive integer.

- If $S \subseteq k^n$, the *ideal of* $S$ is $\mathcal{I}(S) := \{f \in k[x_1,\ldots,x_n] : f(s) = 0 \ \forall\ s \in S\}$. $\mathcal{I}(S)$ is a radical ideal in $k[x_1,\ldots,x_n]$.
- If $I \subseteq k[x_1,\ldots,x_n]$ is an ideal, then the *variety of* $I$ in $k^n$ is $\mathcal{V}(I) := \{s \in k^n : f(s) = 0 \ \forall\ f \in I\}$.
- If $S \subseteq k^n$, then $\mathcal{V}(\mathcal{I}(S))$ is the smallest variety containing $S$ and is called the *Zariski closure* of $S$, denoted as $\overline{S}$.
- Hilbert's Nullstellensatz: If $k$ is algebraically closed and $I$ is an ideal in $k[x_1,\ldots,x_n]$ then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, where $\sqrt{I}$ is the radical of $I$.

(a) If $I$ and $J$ are ideals in $k[x_1,\ldots,x_n]$, the *ideal quotient* of $I$ by $J$ is

$$I : J = \{f \in k[x_1,\ldots,x_n] : fg \in I \ \forall\ g \in J\}.$$

You may use without proof the fact that $I : J$ is an ideal in $k[x_1,\ldots,x_n]$ containing $I$.

Compute $\langle xz, yz\rangle : \langle z\rangle$ in $k[x,y,z]$.

(b) Compute $\mathcal{V}(\langle xz, yz\rangle)$, $\mathcal{V}(\langle z\rangle)$ and $\mathcal{V}(\langle xz, yz\rangle : \langle z\rangle)$.

(c) Let $I$ and $J$ be ideals in $k[x_1,\ldots,x_n]$.

(i) Prove that $\mathcal{V}(I : J) \supseteq \overline{\mathcal{V}(I)\backslash\mathcal{V}(J)}$.

(ii) If $k$ is algebraically closed and $I = \sqrt{I}$ then prove that $\mathcal{V}(I : J) = \overline{\mathcal{V}(I)\backslash\mathcal{V}(J)}$. (Check this statement in the example from parts (a) and (b).)

# Algebra Preliminary Exam

September 8, 2008

**Instructions:** *Do as many problems as you can. Single complete solutions are better than several partial solutions; correct answers to four problems are sufficient to pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Let $f(x)$ be an irreducible polynomial of degree 5 over the field $\mathbb{Q}$ of rational numbers with exactly 3 real roots.
   (a) Show that $f(x)$ is not solvable by radicals.
   (b) Let $E$ be the splitting field of $f$ over $\mathbb{Q}$. Construct a Galois extension $K$ of degree 2 over $\mathbb{Q}$ lying in $E$ such that *no* field $F$ strictly between $K$ and $E$ is Galois over $\mathbb{Q}$.

2. Let $F$ be a finite field. Show for any positive integer $n$ that there are irreducible polynomials of degree $n$ in $F[x]$.

3. Show that the order of the group $GL_n(\mathbb{F}_q)$ of invertible $n \times n$ matrices over the field $\mathbb{F}_q$ of $q$ elements is given by $(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$.

4. By looking at degrees of polynomials, show that any $\mathbb{C}$-subalgebra of the ring $\mathbb{C}[x]$ of polynomials in one variable over the complex field $\mathbb{C}$ is finitely generated.

5.(a) Let $R$ be a commutative principal ideal domain. Show that any $R$-module $M$ generated by two elements takes the form $R/(a) \oplus R/(b)$ for some $a, b \in R$. What more can you say about $a$ and $b$?
   (b) Give a necessary and sufficient condition for two direct sums as in part (a) to be isomorphic as $R$-modules.

**-over-**

6. Let $G$ be the subgroup of $GL_3(\mathbb{C})$ generated by the three matrices

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, C = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

where $i^2 = -1$. Here $\mathbb{C}$ denotes the complex field.

(a) Compute the order of $G$.

(b) Find a matrix in $G$ of largest possible order (as an element of $G$) and compute this order.

(c) Compute the number of elements in $G$ with this largest order.

7.(a) Let $G$ be a group of (finite) order $n$. Show that any irreducible left module over the group algebra $\mathbb{C}G$ has complex dimension at most $\sqrt{n}$.

(b) Give an example of a group $G$ of order $n \geq 5$ and an irreducible left module over $\mathbb{C}G$ of complex dimension $\lfloor \sqrt{n} \rfloor$, the greatest integer to $\sqrt{n}$.

8. Use the rational canonical form to show that any square matrix $M$ over a field $k$ is similar to its transpose $M^t$, recalling that $p(M) = 0$ for some $p \in k[t]$ if and only if $p(M^t) = 0$.

# Algebra Prelim

September 7, 2007

Do as many of the eight problems as you can. Four completely correct solutions will be a pass; a few complete solutions will count more than many partial solutions. Always carefully justify your answers. If you skip a step or omit some details in a proof, point out the gap and, if possible, indicate what would be required to fill it in.

The letters $k$ and $K$ always denote fields.

1. Let $K$ be a field of characteristic zero and $L$ a Galois extension of $K$. Let $f$ be an irreducible polynomial in $K[x]$ of degree 7 and suppose $f$ has no zeroes in $L$. Show that $f$ is irreducible in $L[x]$.

2. Let $K$ be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree $n$. Let $L$ be a splitting field for $f$. Let $G$ be the group of automorphisms of $L$ which act trivially on $K$.

   (a) Show that $G$ embeds in the symmetric group $S_n$.

   (b) For each $n$, give an example of a field $K$ and polynomial $f$ such that $G = S_n$.

   (c) What are the possible groups $G$ when $n = 3$? Justify your answer.

3. Show there are exactly two groups of order 21 up to isomorphism.

4. (a) Show that the ring $\mathbb{Z}[i]$ of Gaussian integers is a unique factorisation domain (UFD).

   (b) Is $\mathbb{Z}[\sqrt{-5}]$ a UFD? Justify your answer.

5. Let $A$ be a domain and $K$ its field of fractions. Recall that we say $f \in K$ is *integral over* $A$ if it satisfies an equation

$$f^n + a_{n-1}f^{n-1} + \cdots + a_1 f + a_0 = 0,$$

where $a_{n-1}, \ldots, a_0 \in A$. The *integral closure* $\tilde{A} \subset K$ of $A$ is the set of $f \in K$ which are integral over $A$, and we say $A$ is *integrally closed* if $\tilde{A} = A$.

   (a) Show that a UFD is integrally closed. (Hint: write $f$ as a fraction.)

   (b) Compute the integral closure of $k[x, y]/(x^2 - y^3)$. (Remember that a polynomial ring is a UFD and therefore integrally closed.)

   (c) Compute the integral closure of $k[x, y, z]/(x^2 - y^2 z)$. (Hint: there is an obvious integral element.)

6. Let $V$ be a finite dimensional vector space over $\mathbb{Q}$ and $A\colon V \to V$ a linear map such that $A^7 = \mathrm{id}$, the identity map. Suppose that 1 is not an eigenvalue of $A$. Prove that $\dim V$ is divisible by 6.

7. Let $V$ be a vector space over a field $k$ that is not of characteristic two. Let $\omega\colon V \times V \to k$ be a non-degenerate skew-symmetric bilinear form, i.e., $\omega(x, y) = -\omega(y, x)$ for all $x, y \in V$, and if $x \neq 0$ there is a $y$ such that $\omega(x, y) \neq 0$.

   (a) Show that there exists a basis $e_1, \ldots, e_n, f_1, \ldots, f_n$ of $V$ such that $\omega(e_i, e_j) = \omega(f_i, f_j) = 0$ and $\omega(e_i, f_j) = \delta_{ij}$ for all $i, j$. (In particular $\dim V = 2n$ is even.)

   (b) We say a subspace $W \subset V$ is *isotropic* if $\omega(w_1, w_2) = 0$ for all $w_1, w_2 \in W$. Show that the dimension of an isotropic subspace is at most $\frac{1}{2}\dim V$.

8. Let $\mathbb{H}$ be the ring of quaternions with standard basis $1, i, j, k$ and identify $\mathbb{C}$ with the subring $\mathbb{R} + \mathbb{R}i$ of $\mathbb{H}$.

   (a) Use the action of $\mathbb{H}$ on itself by left multiplication to explain why there is a ring homomorphism $\varphi : \mathbb{H} \to M_2(\mathbb{C})$, where $M_2(\mathbb{C})$ denotes the ring of $2 \times 2$ matrices. (Warning: there are two ways to view $\mathbb{H}$ as a $\mathbb{C}$-vector space, through right and left multiplication by elements in the subring $\mathbb{R} + \mathbb{R}i$.)

(b) Say why $\varphi$ is injective.

(c) The special unitary group SU(2) consists of all $2 \times 2$ complex matrices $u$ such that $\det(u) = 1$ and $uu^* = u^*u = 1$ where $u^*$ is the conjugate transpose, i.e., the transpose of the matrix whose entries are the complex conjugates of the entries in $u$. Show that $\varphi$ restricts to an isomorphism between the group of unit quaternions (those of length one) and SU(2).

(d) Use this to prove that SU(2) acts transitively on the Riemann sphere $\mathbb{CP}^1$ defined as the 1-dimensional subspaces in $\mathbb{C}^2$. (Hint: use the action of $M_2(\mathbb{C})$ on $\mathbb{C}^2$ by left multiplication.)

(e) Let $U(1)$ denote the image in SU(2) of the multiplicative subgroup of $\mathbb{C} - \{0\}$ consisting of the complex numbers $z \in \mathbb{C} \subset \mathbb{H}$ of length one. Show that the coset space $\mathrm{SU}(2)/U(1)$ is isomorphic to the 2-sphere $S^2$.

Remark. The solution to this problem gives a realization of the Hopf fibration $S^3 \to S^2$ with fibers $S^1$ because the group of unit quaternions is isomorphic to the 3-sphere $S^3$.

**Algebra Preliminary Exam.** **September 2006**

**Instructions:** *Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems are a clear pass. Do not reprove major theorems unless asked to do so, but when you use such theorems, say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

**1.** Let $\mathbf{Z}$ be the ring of integers and let $\{0\}$ be the trivial $\mathbf{Z}$-module. Let $G$ be a finitely generated $\mathbf{Z}$-module, i.e., a finitely generated Abelian group. Show that if $G \otimes_{\mathbf{Z}} F = \{0\}$ for all fields $F$, then $G = \{0\}$.

**2.** Let $c$ be an automorphism of order 1 or 2 of a field $F$. Suppose that $c$ has the property that for any finite set $\{a_j\}_{j\in J}$ of nonzero elements of $F$, $\Sigma_{j\in J} a_j c(a_j)$ is nonzero. For any $n \times n$-matrix $A = (a_{ij})$ with entries in $F$, let $A^c = (c(a_{ij}))$. The $n \times n$ identity matrix is denoted by $I_n$.

Show that if $A$ has the property that $A(A^c)^T = I_n$, then every eigenvalue $\lambda \in F$ for $A$ satisfies the equation $\lambda c(\lambda) = 1$.

(Remark: This result implies the familiar facts that the eigenvalues of an orthogonal matrix over the field of real numbers are in the set $\{\pm 1\}$ and that the eigenvalues of a unitary matrix over the complex numbers have absolute value 1. One takes $c$ to be the identity map in the first case, complex conjugation in the second.)

**3.** (a). Let $p < q < r$ be prime integers. Show that a group of order $pqr$ cannot be simple.

(b). Consider groups of orders $2^2 \cdot 3 \cdot p$ where $p$ has the values 5,7 and 11. For each of those values of $p$, either display a simple group of order $2^2 \cdot 3 \cdot p$, or show that there cannot be a simple group of that order.

**4.** Let $K/F$ be a finite Galois extension and let $n = [K : F]$. There is a theorem (often referred to as the "normal basis theorem") which states that there exists an irreducible polynomial $f(x) \in F[x]$ whose roots form a basis for $K$ as a vector space over $F$. You may assume that theorem in this problem.

(a) Let $G = Gal(K/F)$. The action of $G$ on $K$ makes $K$ into a finite-dimensional representation space for $G$ over $F$. Prove that $K$ is isomorphic to the regular representation for $G$ over $F$.

(The regular representation is defined by letting $G$ act on the group algebra $F[G]$ by multiplication on the left.)

(b) Suppose that the Galois group $G$ is cyclic and that $F$ contains a primitive $n$-th root of unity. Show that there exists an injective homomorphism $\chi : G \to F^\times$.

(c) Show that $K$ contains a nonzero element $a$ with the following property:

$$g(a) = \chi(g) \cdot a$$

for all $g \in G$.

(d) If $a$ has the property stated in (c), show that $K = F(a)$ and that $a^n \in F^\times$.

**5.** Let $G$ be the group of matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ with entries in the finite field $\mathbf{F}_p$ of $p$ elements, where $p$ is a prime.

(a). Prove that $G$ is nonabelian.

(b). Suppose $p$ is odd. Prove that $g^p = I_3$ for all $g \in G$.

(c). Suppose that $p = 2$. It is known that there are exactly two nonabelian groups of order 8, up to isomorphism: the dihedral group $D_4$ and the quaternionic group. Assuming this fact without proof, determine which of these groups $G$ is isomorphic to.

**6.** Let $R = \mathbf{Z}[x]$, the polynomial ring in a variable $x$ with coefficients in the integers.

(a). Let $M$ be a maximal ideal of $R$. Show that $R/M$ is a finite field.

(b). Suppose that $k$ is any finite field. Prove that there exists at least one and no more than a finite number of maximal ideals $M$ such that $R/M \simeq k$.

(c). Prove that no maximal ideal of $R$ is principal, but that all nonmaximal prime ideals of $R$ are principal.

**7.** There are five nonisomorphic groups of order 8. For each of those groups $G$, find the smallest positive integer $n$ such that there is an injective homomorphism $\phi : G \to S_n$.

**8.** Let $K$ be the field $\mathbf{Q}(z)$ of rational functions in a variable $z$ with coeffients in the rational field $\mathbf{Q}$. Let $n$ be a positive integer. Consider the polynomial $x^n - z \in K[x]$.

(a). Show that the polynomial $x^n - z$ is irreducible over $K$.

(b). Describe the splitting field of $x^n - z$ over $K$.

(c). Determine the Galois group of the splitting field of $x^5 - z$ over the field $K$.

Algebra Preliminary Exam September 2005

Instructions: Do as many problems as you can. Single complete solutions are better than several partial solutions. Correct answers to four problems is a pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.

1. For any group $G$ we define $\Omega(G)$ to be the image of the group homomorphism $\rho : G \to \mathrm{Aut}(G)$ where $\rho$ maps $g \in G$ to the conjugation automorphism $x \to gxg^{-1}$. Starting with a group $G_0$, we define $G_1 = \Omega(G_0)$ and $G_{i+1} = \Omega(G_i)$ for all $i \geq 1$. If $G_0$ is of order $p^e$ for a prime $p$ and integer $e \geq 2$, prove that $G_{e-1}$ is the trivial group.

2. Let $\mathbb{F}_2$ be the field with 2 elements.

(a) What is the order of $GL_3(\mathbb{F}_2)$?

(b) Use the fact that $GL_3(\mathbb{F}_2)$ is a simple group (which you should not prove) to find the number of elements of order 7 in $GL_3(\mathbb{F}_2)$.

3. Let $G$ be a finite abelian group. Let $f : \mathbb{Z}^m \to G$ be a surjection of abelian groups. We may think of $f$ as a homomorphism of $\mathbb{Z}$-modules. Let $K$ be the kernel of $f$.

(a) Prove that $K$ is isomorphic to $\mathbb{Z}^m$.

(b) We can therefore write the inclusion map $K \to \mathbb{Z}^m$ as $\mathbb{Z}^m \to \mathbb{Z}^m$ and represent it by an $m \times m$ integer matrix $A$. Prove that $|\det A| = |G|$.

4. Let $R = C([0,1])$ be the ring of all continuous real-valued functions on the closed interval $[0,1]$, and for each $c \in [0,1]$, denote by $M_c$ the set of all functions $f \in R$ such that $f(c) = 0$.

(a) Prove that $g \in R$ is a unit if and only if $g(c) \neq 0$ for all $c \in [0,1]$.

(b) Prove that for each $c \in [0,1]$, $M_c$ is a maximal ideal of $R$.

(c) Prove that if $M$ is a maximal ideal of $R$, then $M = M_c$ for some $c \in [0,1]$. (Hint: compactness of $[0,1]$ may be relevant.)

5. Let $R$ and $S$ be commutative rings, and $f : R \to S$ a ring homomorphism.

(a) Show that if $I$ is a prime ideal of $S$, then

$$f^{-1}(I) = \{r \in R : f(r) \in I\}$$

is a prime ideal of $R$.

(b) Let $N$ be the set of nilpotent elements of $R$:

$$N = \{r \in R : r^m = 0 \text{ for some } m \geq 1\}.$$

$N$ is called the nilradical of $R$. Prove that it is an ideal which is contained in every prime ideal.

(c) Part (a) lets us define a function

$$\begin{aligned} f^* : \{\text{prime ideals of } S\} &\longrightarrow \{\text{prime ideals of } R\}. \\ I &\longmapsto f^{-1}(I) \end{aligned}$$

Let $N$ be the nilradical of $R$. Show that if $S = R/N$ and $f : R \to R/N$ is the quotient map, then $f^*$ is a bijection.

6. Let $F$ be a finite field of characteristic $p$. Let $A$ be an $n \times n$ matrix over $F$. Suppose that $A^p$ is the identity matrix. Show that for every polynomial $f(x)$, the characteristic polynomial of the matrix $f(A)$ is equal to $(t-c)^n$ for some $c$.

7. Consider the polynomial $f(x) = x^{10} + x^5 + 1 \in \mathbb{Q}[x]$ with splitting field $K$ over $\mathbb{Q}$.

(a) Determine whether $f(x)$ is irreducible over $\mathbb{Q}$ and find $[K : \mathbb{Q}]$.

(b) Determine the structure of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

8. For each prime number $p$ and each positive integer $n$, how many elements $\alpha$ are there in $\mathbb{F}_{p^n}$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^6}$?

**Algebra Preliminary Exam** **September 2004**

**Instructions:** *Do as many problems as you can. Single complete solutions are better than several partial solutions; correct answers to four problems are usually sufficient to pass. Do not reprove major theorems unless asked to do so, but when you use such theorems say so. In writing down partial solutions try to indicate the gaps as clearly as possible, so that we can see what you do and don't know.*

1. Characterize the set of prime numbers $p$ such that any group of order $17p$ is abelian.

2.(a) Let $L$ be a Galois extension of a field $K$ of degree 4. Work out all the possibilities for the number $n$ of fields lying strictly between $K$ and $L$.

(b) Using the Galois correspondence, give an example of a *non*-Galois extension $L$ of a field $K$ of degree 4 such that there are no fields strictly between $L$ and $K$.

3.(a) Let $R$ be a commutative ring and $M$ an $R$-module. Suppose that $M$ has a submodule $N$ such that both $N$ and $M/N$ are free as $R$-modules. Show that $M$ is free as an $R$-module and compute its rank as a function of the ranks of $N$ and $M/N$.

(b) Give an example of a commutative ring $R$, a free $R$-module $M$, and a submodule $N$ such that neither $N$ nor $M/N$ is free as an $R$-module.

4. Let $G$ be a group of order 80 with a subgroup $H$ of order 16. By looking at the action of $G$ on left cosets of $H$, show that $G$ has a nontrivial normal subgroup.

5. Let $K, L$ be a finite fields of the same characteristic and $K^*, L^*$ their multiplicative groups of nonzero elements. Show that there is an injective group homomorphism from $K^*$ into $L^*$ if and only if there is an injective field homomorphism from $K$ into $L$. Give a simple condition on the orders of $K$ and $L$ for such homomorphisms to exist.

-over-

6. Let $R$ be a principal ideal domain with field of fractions $K$. Let $K^*, U$ be the multiplicative groups of nonzero elements of $K$ and units in $R$, respectively. Show that the quotient $K^*/U$ is a free abelian group and give a natural set of generators for it.

7.(a) Let $L$ be a finite Galois extension of a field $K$ whose Galois group $G$ is cyclic of order $n$. Assume that $K$ has $n$ distinct $n$th roots of 1. Letting $g$ be a generator of $G$, determine the characteristic polynomial of $g$ as a $K$-linear map from the vector space $L$ to itself.

(b) Find the roots of this characteristic polynomial.

(c) Show that $g$ has $n$ distinct eigenvalues in $K$, each with multiplicity one.

(d) In particular, there is $x \in L, x \neq 0$ and $\alpha \in K$, $\alpha$ a primitive $n$th root of 1, with $gx = \alpha x$. Show that $x^n \in K$ and that $L$ is generated over $K$ by $x$.

8. A *variety* is the set of common zeros in $\mathbb{C}^n$ of some collection $\mathcal{C}$ of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. Show that any variety $\mathcal{V}$ is in fact the set of common zeros of some *finite* collection of polynomials in $\mathbb{C}[x_1, \ldots, x_n]$.

**Algebra Preliminary Exam** **September 2003**

**Instructions.** Do as many problems as you can. No one is expected to solve all the problems. Complete solutions are better than partial solutions; correct answers to four problems are usually sufficient to pass. Do not reprove major theorems unless asked to, but when you use such theorems say so. Aim for clarity; even when you don't know something it is helpful if you can say that clearly so we see that you know what you do and don't know.

**Notation.** The letters $F$, $k$, and $K$, will always denote fields. We write $\mathbb{F}_q$ for the field with $q$ elements, and $GL_n(R)$ for the group of invertible $n \times n$ matrices with entries in a commutative ring $R$. We write $\mathbb{Z}_n$ for the quotient $\mathbb{Z}/n\mathbb{Z}$ viewed as both an abelian group under addition and as a ring.

**Terminology.** Matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \qquad \begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & C \end{pmatrix},$$

where $A, B, C$ are square matrices, and so on, are called block diagonal matrices.

(1) Let $G$ be a group with $992 = 2^5 \times 31 = 32 \times 31$ elements.
   (a) Show that $G$ has a proper normal subgroup.
   (b) Does there exist a group of order 992 that does NOT have a normal subgroup of order 31?

   HINT: The number of elements in $GL_n(\mathbb{F}_q)$ is $(q^n-1)(q^n-q)\dots(q^n-q^{n-1})$.

(2) Let $R$ be a commutative noetherian domain.
   (a) Prove that every non-invertible element of $R$ can be written as a product of irreducible elements.
   (b) Let $K$ be the field of fractions (quotient field) of $R$. Suppose that for every element $x \in K$ either $x$ or $x^{-1}$ belongs to $R$. Show that $R$ has a unique maximal ideal and that every ideal of $R$ is principal. HINT: focus on $\{x \in R \mid x^{-1} \notin R\}$; if $x, y \in R$ the hypothesis implies that either $x/y$ or $y/x$ is in $R$; you can use the result of part (a) if you wish and/or Nakayama's Lemma provided you state it correctly.

(3) (a) Prove that $\mathbb{Z}[x]/(2x-1, x^7-1) \cong \mathbb{Z}/(127)$.
   (b) Prove that $\mathbb{Z}[i]/(2i-3) \cong \mathbb{F}_{13}$.

(4) Let $R$ be a commutative domain.
   (a) Define a torsion module over $R$.
   (b) Define a torsion-free module over $R$.
   (c) State the classification theorem for finitely generated modules over a principal ideal domain. Your statement of this theorem should allow one to determine whether two such modules are isomorphic.
   (d) Let $M$ be an $n \times n$ matrix with entries in the field $k$ regarded as an endomorphism of $V = k^n$. Suppose that M is NOT conjugate to a block diagonal matrix. Show there is a vector $v \in V$ for which $\{M^i v \mid i \geq 0\}$ spans $V$.

(5) Let $R$ be a ring with the following properties:
- up to isomorphism $R$ has three distinct simple left modules, $S_1$, $S_2$, and $S_3$;
- the endomorphism rings of these modules are $\mathrm{End}_R S_1 \cong \mathbb{R}$, $\mathrm{End}_R S_2 \cong \mathbb{C}$, $\mathrm{End}_R S_3 \cong \mathbb{H}$, the ring of quaternions;
- every left $R$-module is a direct sum of simple modules.

(a) Describe explicitly the structure of the ring $R$.
(b) Express $R$ as a direct sum of simple left $R$-modules.

(6) (a) Define what is meant by a composition series for a module.
(b) Define length of a module.
(c) State the result that ensures your definition in (b) makes sense.
(d) Let $M$ be a module of length two over a ring $R$. Show that either $M$ has a unique simple submodule or is a direct sum of two simple modules.
(e) Give examples showing that both possibilities in (d) can occur. Be certain to say what the ring is as well as what the module is.

(7) Let $p(x) = x^3 - 5 \in K[x]$ and let $F$ be a splitting field for $p$ over $K$.
(a) What are the possible Galois groups $G = \mathrm{Gal}(F/K)$? Give reasons.
(b) For each possible $G$ describe a field $K$ such that $G = \mathrm{Gal}(F/K)$.

(8) (a) Let $G$ a finite group of automorphisms of a field $K$, and $F$ the subfield fixed by $G$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the orbit of $\alpha = \alpha_1 \in K$. Show that the minimal polynomial of $\alpha$ over $F$ is $g(x) := (x - \alpha_1) \ldots (x - \alpha_n)$.
(b) Let $G = \langle \sigma, \tau \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ be the group generated by the automorphisms $\sigma$ and $\tau$ of the rational function field $\mathbb{C}(t)$ defined by $\sigma(t) = it^{-1}$ and $\tau(t) = -t$. Show that the fixed field of $G$ is the rational function field $\mathbb{C}(z)$ generated by $z = t^2 - t^{-2}$.

**Algebra Prelim** **September 16, 2002**

**Instructions:** *Do as many problems as you can. Complete solutions are preferable to partial results. You should not reprove major theorems, but if you use a major theorem, you should state what you are using clearly. You should write enough so that there is no doubt that you know what is going on, but do not write a book when a few lines suffice.*

**1.** Prove that any group of order 245 must be abelian. Describe all such groups up to isomorphism.

**2.** (a) Let $V$ be a simple module over the polynomial ring $R = \mathbb{R}[x]$, where $\mathbb{R}$ is the field of real numbers. Prove that $V$ is a vector space over $\mathbb{R}$ of dimension 1 or 2.

(b) Suppose that $W$ is a nonzero finite dimensional vector space over $\mathbb{R}$. Let $A$ be a linear transformation of $W$ to itself. (That is, $A \in End_{\mathbb{R}}(W)$.) Prove that there is a subspace $U$ of $W$ of dimension 1 or 2 such that $AU \subset U$.

**3.** (a) Let $G = GL_2(\mathbb{Q})$, where $\mathbb{Q}$ is the field of rational numbers. Prove that $G$ has elements of order 2, 3, 4, and 6, but no elements of order 5.

(b) What is the smallest value of $n$ such that $GL_n(\mathbb{Q})$ has an element of order 5.

**4.** Let $G$ be a finite group of order $6m$, where $(6, m) = 1$. Suppose that $g$ is an element of $G$ of order 3. Prove that $G$ has an element of order 6 if and only if the number of conjugates of $g$ in $G$ is odd.

**5.** Suppose that $R$ is a ring. Consider an exact sequence of $R$-modules:

$$(*) \qquad 0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \longrightarrow 0$$

(Recall that "exactness" means that $f$ is injective, $g$ is surjective, and $\ker(g) = \mathrm{im}(f)$.) We say that the exact sequence (*) splits if there is an $R$-module homomorphism $h : M_3 \to M_2$ such that $g \circ h : M_3 \to M_3$ is the identity map.

(a) Prove that if the exact sequence (*) splits, then $M_2$ is isomorphic to the direct sum $M_1 \oplus M_3$.

(b) Suppose $R$ is the polynomial ring $\mathbb{C}[x, y]$ in two indeterminates $x$ and $y$, where $\mathbb{C}$ is the field of complex numbers. Give an example of an exact sequence (*) of $R$-modules which does not split.

(c) Suppose that $R$ is an integral domain and that every exact sequence (*) of $R$-modules splits. Prove that $R$ is a field.

*(over)*

**6.** Let $R = \mathbb{C}[x,y]/(x^2+y^3)$, where $\mathbb{C}[x,y]$ is the polynomial ring over $\mathbb{C}$ in the indeterminates $x$ and $y$. Let $S$ be the subring $\mathbb{C}[t^2,t^3]$ of $\mathbb{C}[t]$, where $\mathbb{C}[t]$ is the polynomial ring in the indeterminate $t$ over $\mathbb{C}$.

(a) Prove that the rings $R$ and $S$ are isomorphic.

(b) Let $I$ be the ideal in $R$ generated by the residue classes of $x$ and $y$. Prove that $I$ is a prime ideal of $R$, but not a principal ideal.

**7.** Let $F$ be the finite field $\mathbb{Z}/5\mathbb{Z}$, where $\mathbb{Z}$ denotes the ring of integers. Let $K$ be the splitting field over $F$ for the polynomial $f(x) = (x^2-2)(x^3-2)(x^4-2)(x^{31}-1)$. Determine the Galois group $Gal(K/F)$.
(NOTE: It may be helpful to note that 31 divides $5^3-1$.)

**8.** This question concerns the group ring $\mathbb{Z}[G]$ associated to a group $G$. By definition, $\mathbb{Z}[G]$ is the free abelian group which has the set $G$ as a basis. That is, $\mathbb{Z}[G]$ consists of all formal finite sums $\sum_{g\in G} a_g g$, where the coefficients $a_g$ are in $\mathbb{Z}$. One makes $\mathbb{Z}[G]$ into a ring by extending the multiplication operation on $G$ to $\mathbb{Z}[G]$ by the distributive law. As an example, if $G$ is an infinite cyclic group generated by $x$, then $\mathbb{Z}[G]$ is isomorphic to the ring $\mathbb{Z}[x,x^{-1}]$, where $x$ is regarded as an indeterminate.

One basic property is the following: Suppose that $G$ and $H$ are groups. If one has a group homomorphism $f : G \to H$, then one obtains a ring homomorphism $F : \mathbb{Z}[G] \to \mathbb{Z}[H]$ defined by

$$F(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g f(g)\,.$$

You do not need to prove this basic property.

Assume that $G$ is an abelian group. Prove that $\mathbb{Z}[G]$ is a Noetherian ring if and only if $G$ is a finitely generated group.