ALGEBRA QUALIFYING EXAM, SUMMER 2009

1. Groups

You must do problem 1 in this section and you must do *two* of problems 2 through 4.

(1) (a) Find a 2-Sylow subgroup of S_5.
  (b) Find a 5-Sylow sugroup of S_{15}.
  (c) For prime p, how many p-Sylow subgroups does S_p have?
  (d) For prime p, what is the order of the normalizer of a p-Sylow subgroup P in S_p?

(2) (a) State the class equation. normal
  (b) Suppose $|G| = p^k$ and H is a$^\wedge$subgroup of G with $|H| > 1$. Show that H contains a non-identity element of the center $Z(G)$ of G.

(3) Let $|G| = pq$ where p and q are prime, $p < q$.
  (a) Show that G is not a simple group.
  (b) If p does not divide $q - 1$, show that G is abelian.
  (c) If p divides $q - 1$, what are the possibilities for G? (You need not give detailed justification for your answer to part (c).)

(4) If A and B are normal in G, and G/A and G/B are abelian, show that $G/(A \cap B)$ is also abelian.

2. Rings

You must do *three* of the following 4 problems.
Conventions: All rings are rings with 1, and an integral domain is commutative.

(1) For each of the following, either give an example or indicate that none exists. You do not need to supply proofs.
  (a) Two non-zero $\mathbf{Z}$-modules A and B such that $A \otimes_{\mathbf{Z}} B = 0$.
  (b) Two non-zero $\mathbf{Q}$-modules V and W such that $V \otimes_{\mathbf{Q}} W = 0$.
  (c) A ring R and a module M over R which is torsion free but is not free.
  (d) A ring R and an ideal I of R that is maximal but not prime.
  (e) A ring which is not Noetherian.
  (f) A ring whose center is not an ideal.

(2) A ring is called left (resp. right) Artinian if every descending chain of left (resp. right) ideals $I_1 \supset I_2 \supset I_3 \cdots$ eventually terminates (i.e. there is some N such that $I_k = I_N$ for $k \geq N$). A ring is called Artinian if it is both left and right Artinian.
  (a) Let A be a left Artinian ring and suppose that $f \colon A \to R$ is a surjective homomorphism. Prove that R is left Artinian.
  (b) Show that an Artinian integral domain A is a field. (Hint: for a nonzero element $a \in A$, consider the ideals $(a), (a^2), (a^3), \ldots$.)
  (c) Show that every prime ideal in a commutative Artinian ring is maximal.

(3) (a) List all isomorphism classes of groups of size 120.

(b) Find all isomorphism classes of $\mathbf{Q}[x]$ modules V such that $\dim_{\mathbf{Q}} V = 6$ and V is annihilated by $(x-3)^2(x+5)$.

(c) Find all possible rational canonical forms for a 6 by 6 matrix over $\mathbf{Q}$ that has minimal polynomial $(x-3)^2(x+5)$.

(4) Give a complete factorization of each of the following over the indicated rings. Explain why the factors you obtain are irreducible.

(a) $x^5 - 1$ over $\mathbf{C}$.

(b) $x^6 - 1$ over $\mathbf{Q}$.

(c) $x^7 + 3x^5 - 6x^3 + 9x - 15$ over $\mathbf{Q}$.

(d) $x^{11} - x$ over $\mathbf{F}_{11}$.

(e) $x^{13} - x - 1$ over $\mathbf{F}_{13}$.

3. Fields

You must do problem 1 in this section and you must do *two* of problems 2 through 4.

(1) Let K be the splitting field of $x^4 - 4x^2 - 3$ over $\mathbf{Q}$.

(a) What is the dimension of K over $\mathbf{Q}$?

(b) What is the Galois group of K over $\mathbf{Q}$? (Identify the isomorphism type of the Galois group, and also indicate how its elements act as permutations of the roots of f.)

(c) How many subfields does K have of each dimension over $\mathbf{Q}$?

(d) How many subfields of K of each dimension are Galois over $\mathbf{Q}$?

(2) Indicate whether each of the following if-then statements is true, and give a brief explanation to support your answer. If the statement is false, and there is a reasonable addition to the hypotheses that would make it true, please indicate that as well.

(a) If f is an irreducible 4th degree polynomial with rational coefficients then the roots of f are constructible numbers.

(b) If g is an irreducible 6th degree polynomial with rational coefficents then the roots of g are constructible.

(c) If E and F are finite fields and $F \subset E$ then E/F is Galois.

(d) If E/F and K/F are both Galois extensions then EK/F is a Galois extension.

(e) If E and F are finite fields and $|F|$ divides $|E|$ then E has a subfield isomorphic to F.

(3) Let L/K be a Galois extension of fields, with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$, and let $\alpha \in L$. Prove that $L = K(\alpha)$ iff $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are distinct.

(4) (a) Let F be a field and let K be a field containing F. Suppose that $\alpha, \beta \in K$ are both algebraic over F. Prove that $\alpha + \beta$ is algebraic over F.

(b) What is the minimal polynomial of $\sqrt{5} + 2\sqrt{7}$ over $\mathbf{Q}$?

Preliminary exam in algebra
June 11, 2008
9 a.m.-noon

Instructions. This is a closed-book exam. There are three sections, in each of which you should do the two starred problems and one additional problem of your choice. Answers with inadequate explanation will not receive full credit.

I. Groups

*1(a) State Sylow's Theorem.

(b) Prove that no group of order 6545 is simple.

*2(a) Determine the elementary divisors and invariant factors of the Abelian group $\mathbf{Z}_{15} \times \mathbf{Z}_{20} \times \mathbf{Z}_9$ of order 2700.

(b) Determine the number of nonisomorphic Abelian groups of order 2700.

3. Let p be prime, G be a group of order $p^n > 1$, and X be a finite G-set whose size is not divisible by p. Prove that G has a fixed point in X: i.e., an $x \in X$ such that $gx = x$ for all $g \in G$.

4. Let G be a finite group. For any $x \in G$

$$Z_G(x) = \{g \in G : gxg^{-1} = x\}$$

is the centralizer of x in G and

$$x^G = \{gxg^{-1} : g \in G\}$$

is the conjugacy class of x in G.

(a) Show that $|x^G| = [G : Z_G(x)]$.

(b) If $H \leq G$ and $x \in H$, prove that $Z_H(x) = H \cap Z_G(x)$.

(c) If H is a subgroup of index 2 in G and $x \in H$, prove that either $|x^H| = |x^G|$ or $|x^H| = \frac{1}{2}|x^G|$.

II. Rings and modules

*1. There are finitely many 6×6 matrices over $\mathbf{Q}$, in rational canonical form, with minimal polynomial $(x+2)^2(x-1)$. Find them.

*2(a) Show that every Euclidean domain is a principal ideal domain.

In parts (b) and (c) assume that $\mathbf{Z}[i]$ is a Euclidean domain with respect to the norm function N defined by

$$N(a+bi) = a^2 + b^2 \text{ for all } a+bi \in \mathbf{Z}[i].$$

(b) Let I be a nonzero ideal of $\mathbf{Z}[i]$ generated by α. Show that every coset of I in $\mathbf{Z}[i]$ contains an element of norm less than $N(\alpha)$.

(c) Show that $\mathbf{Z}[i]/I$ is finite.

3. A square matrix N over the complex numbers is nilpotent just in case $N^a = 0$ for some positive integer a. Show that every nilpotent N is similar to a matrix of the form

$$\begin{pmatrix} N_1 & & & \\ & N_2 & & \\ & & \ddots & \\ & & & N_s \end{pmatrix}$$

where each N_i is a square matrix of the form

$$\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ & & & 1 & 0 \end{pmatrix}.$$

4. Let R be a principal ideal domain and A and B be finitely generated R-modules. Show that if $A \oplus A \cong B \oplus B$ then $A \cong B$.

III. Fields

*1. Find the Galois groups, over $\mathbf{Q}$, of the following polynomials.

(a) $x^4 - 25$.

(b) $x^3 - x + 1$.

*2. Let F be a field and $g(x) \in F[x]$ have degree $n > 0$.

(a) Define 'E is a splitting field for $g(x)$ over F.'

(b) Prove, without using the Fundamental Theorem of Galois Theory, that if E is a splitting field for $g(x)$ over F then $[E : F] \leq n!$.

3. Find the Galois groups, over $\mathbf{Q}$, of the following polynomials.

(a) $x^4 + 4$.

(b) $x^3 + x^2 - 2x - 1$. Hint: show that if r is a root, then $r^2 - 2$ also is a root.

4. Recall that every finite group G is isomorphic to a subgroup of S_n for some $n > 0$. Show that there are fields $E \supseteq F$ such that the Galois group of E over F is isomorphic to G.

Algebra Preliminary Exam

Solutions

I. Groups

1. a. Sylow's Theorem

   1. Sylow p-subgroups Exist (i.e. $Syl_p(G) \neq \emptyset$)
   2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$. i.e. Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups are conjugate in G.
   3. The number of Sylow p-subgroups is of the form $1+kp$, in other words, $n_p \equiv 1(modp)$. Further, n_p is the index in G of the normalizer $N_G(p)$ for any Sylow p-subgroup P. Hence n_p divides m.

   b. G a group, with $\mid G \mid = 6545 = 5 \cdot 7 \cdot 11 \cdot 17$. A simple group is one which has no non-trivial normal subgroups. Suppose that G is simple, so any non-trivial Sylow p-subgroup P of G will not be normal in G, meaning $n_p \neq 1$. First Examine the Sylow 7-subgroups. By Sylow's Theorem, we know $n_7 \mid 11 \cdot 5 \cdot 17$ and $n_7 \equiv 1(mod7)$. Therefore, it must be the case that $n_7 = 85$.

   Now, let's examine the Sylow 11-subgroups. By Sylow's Theorem, we know $n_{11} \mid 5 \cdot 7 \cdot 17$ and $n_{11} \equiv 1(mod11)$. Therefore, it must be the case that $n_{11} = 595 = 5 \cdot 7 \cdot 11$.

   Now let's examine the Sylow 5-subgroups. By Sylow's Theorem, we know $n_5 \mid 11 \cdot 7 \cdot 17$ and $n_5 \equiv 1(mod5)$. Therefore, it must be the case that $n_5 = 11$.

   Finally, let's examine the Sylow 17-subgroups. By Sylow's Theorem, we know $n_{17} \mid 11 \cdot 7 \cdot 5$ and $n_{17} \equiv 1(mod17)$. Therefore, it must be the case that $n_{17} = 34$.

   Now we know the number of Sylow p-subgroups for each factor of 6545, and using these values we can compute the total number of elements in G:

$$\begin{aligned} \mid G \mid &= 85(7-1) + 595(11-1) + 11(5-1) + 34(17-1) + 1 \\ &= 85(6) + 595(10) + 11(4) + 34(16) + 1 \\ &= 510 + 5950 + 44 + 544 + 1 \\ &= 7049 \\ &> 6545 \end{aligned}$$

   Thus we have reached a contradiction. Hence the number of Sylow p-subgroups for some p must be equal to 1, meaning that at least one of the Sylow p-subgroups is normal in G. Therefore G is not simple.

2. a. G a group, G=$\mathbf{Z}_{15} \times \mathbf{Z}_{20} \times \mathbf{Z}_9$. If gcd(a,b)=1, then $\mathbf{Z}_a \times \mathbf{Z}_b \cong \mathbf{Z}_{ab}$, therefore we may conclude that

$$\mathbf{Z}_{15} \times \mathbf{Z}_{20} \times \mathbf{Z}_9 \cong \mathbf{Z}_{15} \times \mathbf{Z}_{180}$$

   However, two groups are isomorphic just in case they have the same rank and list of invariant factors, so we may conclude that the invariant factors of G are 15 and

180. In addition, we know

$$\mathbf{Z}_{180} \cong \mathbf{Z}_{3^2} \times \mathbf{Z}_{2^2} \times \mathbf{Z}_5$$
$$\mathbf{Z}_{15} \cong \mathbf{Z}_3 \times \mathbf{Z}_5$$

Therefore the elementary divisors of G are 3,5,3^2,2^2,5.

b. Too long to write out. Just think about it.

3. Let p be prime, G a group of order p^n, and X a finite G-set whose size is not divisible by p. For any $x_i \in X$ we define the orbit of x_i in G as

$$\mathcal{O}(x_i) = \{gx_i : g \in G\}$$

Note, for any $x_i \in X$, $\mid \mathcal{O}(x_i) \mid = [G : G_{x_i}]$. So suppose no x_i is fixed, this would mean $\mid \mathcal{O}(x_i) \mid \neq 1$ for any x_i. By Lagrage's Theorem, we know

$$\begin{aligned}
&[G : G_{x_i}] \mid \mid G \mid \\
\Longrightarrow &[G : G_{x_i}] = p^{k_i} \\
\Longrightarrow &\sum_{i=1}^{m} [G : G_{x_i}] = p^{k_1} + p^{k_2} + ... + p^{k_m} \\
\Longrightarrow &\sum_{i=1}^{m} \mid \mathcal{O}(x_i) \mid = p^{k_1} + p^{k_2} + ... + p^{k_m}
\end{aligned}$$

But orbits are the disjoint equivalence classes formed by G acting on X, so in fact

$$\begin{aligned}
&\sum_{i=1}^{m} \mid \mathcal{O}(x_i) \mid = \mid X \mid \\
\Longrightarrow &\mid X \mid = p^{k_1} + p^{k_2} + ... + p^{k_m} \\
\Longrightarrow &p \mid\mid X \mid
\end{aligned}$$

Therefore we have reached a contradiction, hence for some i, $\mid \mathcal{O}(x_i) \mid$ must equal 1, meaning some x_i must be fixed.

4. Let G be a finite group. For any $x \in G$

$$Z_G(x) = \{g \in G : gxg^{-1} = x\}$$

is the centralizer of x in G and

$$x^G = \{gxg^{-1} : g \in G\}$$

is the conjugacy class of x in G.

a. We wish to show that $\mid x^G \mid = [G : Z_G(x)]$. For any set A being acted on by G (in this case, by conjugation), for any $a \in A$, the size of the equivalence class (in this case, the conjugacy class) containing a is $[G : G_a]$ where $G_a = \{g \in G : gag^{-1} = a\} = N_G(a)$. For a single element x in the G-set X,

$$G_x = \{g \in G : gxg^{-1} = x\} = N_G(\{x\}) = Z_G(x)$$

Therefore,

$$\mid x^G \mid = [G : G_x] = [G : Z_G(x)]$$

b. Suppose $H \leq G$ and $x \in H$. We wish to show that $Z_H(x) = H \cap Z_G(x)$. First, suppose $h \in Z_H(x)$.

$$\begin{aligned}
&\Longrightarrow h \in \{h \in H : hxh^{-1} = x\} \text{ and since } H \leq G, h \in G\\
&\Longrightarrow h \in H \text{ and } h \in \{g \in G : gxg{-}1 = x\}\\
&\Longrightarrow h \in H \cap \{g \in G : gxg^{-1} = x\}\\
&\Longrightarrow h \in H \cap Z_G(x)\\
&\Longrightarrow Z_H(x) \subseteq H \cap Z_G(x)
\end{aligned}$$

Now suppose $h \in H \cap Z_G(x)$.

$$\begin{aligned}
&\Longrightarrow h \in H \text{ and } h \in \{g \in G : gxg{-}1 = x\}\\
&\Longrightarrow h \in H \text{ and } hxh^{-1} = x\\
&\Longrightarrow h \in \{h \in H : hxh{-}1 = x\}\\
&\Longrightarrow h \in Z_H(x)\\
&\Longrightarrow H \cap Z_G(x) \subseteq Z_H(x)
\end{aligned}$$

Therefore we may conclude that $Z_H(x) = H \cap Z_G(x)$.

c. Suppose $H \leq G, [G : H] = \frac{|G|}{|H|} = 2, x \in H$. By part (a), we know

$$\mid x^H \mid = [H : Z_H(x)] = \frac{\mid H \mid}{\mid Z_H(x) \mid}$$

and

$$\mid x^G \mid = [G : Z_G(x)] = \frac{\mid G \mid}{\mid Z_G(x) \mid}$$

Now it follows,

$$2 = \frac{\mid G \mid}{\mid H \mid} = \frac{\mid x^G \mid \cdot \mid Z_G(x) \mid}{\mid x^H \mid \cdot \mid Z_H(x) \mid}$$

But note, $Z_H(x) \leq Z_G(x)$, since for $h_1, h_2 \in Z_H(x)$

$$\begin{aligned}
&h_1xh_1^{-1} = x, h_2xh_2^{-1} = x\\
&\Longrightarrow h_1h_2x(h_1h_2)^{-1} = h_1h_2xh_2^{-1}h_1^{-1} = h_1(h_2xh_2^{-1})h_1^{(} - 1) = h_1xh_1^{-1} = x\\
&\Longrightarrow Z_H(x) \leq Z_G(x)
\end{aligned}$$

Now this means $\mid Z_H(x) \mid\mid\mid Z_G(x) \mid$. Now we may examine cases:

Case-I Suppose $\mid Z_H(x) \mid = \mid Z_G(x) \mid$

$$\Longrightarrow 2 = \frac{\mid x^G \mid}{\mid x^H \mid} \cdot 1$$
$$\Longrightarrow 2 \cdot \mid x^H \mid = \mid x^G \mid$$

Therefore, $\mid x^H \mid = \frac{1}{2} \cdot \mid x^G \mid$

Case-II Suppose $\mid Z_H(x) \mid \neq \mid Z_G(x) \mid$

Then

$$[\mid Z_G(x) \mid : \mid Z_H(x) \mid] = \frac{\mid Z_G(x) \mid}{\mid Z_H(x) \mid} > 1$$

and we know

$$\frac{\mid x^G \mid}{\mid x^H \mid} \geq 1$$

So the only possible choice to have the product equal 2, is if

$$\frac{\mid x^G \mid}{\mid x^H \mid} = 1$$

which means

$$\mid x^G \mid = \mid x^H \mid$$

II. Rings and Modules

1. If $(x+2)^2(x-1)$ is the minimal polynomial for a matrix, this means all invariant factors must divide this. Furthermore, the characteristic polynomial for this matrix, which is the product of all invariant factors, must be a degree-6 polynomial. This gives is the following choices for list of invariant factors, and the corresponding rational canonical form:

i.

$$(x+2)^2(x-1), (x+2)^2(x-1) \qquad \begin{bmatrix} 0 & 0 & 4 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

ii.

$$(x+2)^2(x-1), (x+2)^2, (x+2) \qquad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

iii.

$$(x+2)^2(x-1), (x+2)(x-1), (x+2) \qquad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

iv.

$$(x+2)^2(x-1), (x+2)(x-1), (x-1) \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

v.

$$(x+2)^2(x-1), (x+2), (x+2), (x+2) \qquad \begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

vi.

$$(x+2)^2(x-1), (x-1), (x-1), (x-1) \qquad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

2. a. We wish to show that every ideal in a Euclidean Domain is generated by a single element. Let R be a Euclidean Domain, and I an ideal of R. If I is a zero ideal, clearly it is principal, and we are done. Suppose I is not the trivial ideal. Then I contains a non-zero element d of minimum norm. The ideal generated by this element is $(d) = \{rd : r \in R\}$. However, since I is an ideal, and $d \in R$, by definition of ideal, we may conclude $(d) \subseteq I$. Now pick any arbitrary $a \in R$. Since R is a Euclidean domain, and $a, d \in R$ we know there exist elements $q, r \in R$ such that $a = qd+r$ where $N(r) = 0$ or $N(r) < N(d)$. However, we picked d to be the element of minimum norm, hence $N(r) = 0$, which implies $a = qd$, and hence $a \in (d)$. Therefore, $I = (d)$, so any ideal in R is principal and thus R is a Principal Ideal Domain.

b. Suppose $\mathbb{Z}[i]$ is a Euclidean domain with respect to the norm

$$N(a+bi) = a^2 + b^2 \qquad \forall a+bi \in \mathbb{Z}[i]$$

Let I be a nonzero ideal of $\mathbb{Z}[i]$ generated by $\alpha \in \mathbb{Z}[i]$. We wish to show that every coset of I in $\mathbb{Z}[i]$ contains an element of norm less than $N(\alpha)$. We know

$$(\alpha) = \{(a+bi)\alpha : a+bi \in \mathbb{Z}[i]\}$$

and any coset of (α) in $\mathbb{Z}[i]$ looks like

$$(x+iy) + (\alpha)$$

for some fixed $x+iy \in \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Euclidean Domain we have the division algorithm in R, so for any elements α and $x+iy$ in $\mathbb{Z}[i]$ there exist elements q and r in $\mathbb{Z}[i]$ such that

$$x+iy = q\alpha + r$$

where $N(r) = 0$ or $N(r) < N(\alpha)$. However, in this case

$$r = x+iy+(-q)\alpha$$

which is just an element of the coset of (α) in $\mathbb{Z}[i]$ containing $x+iy$. We know either $N(r) = 0$ or $N(r) < N(\alpha)$, but since we picked α to be nonzero, in either case the norm of r is less than the norm of α.

c. Suppose $N(\alpha) = n \in \mathbb{Z}$. Since every coset of I in $\mathbb{Z}[i]$ contains an element of norm less than the norm of α it is only possible to have n cosets, which is clearly finite.

3. A square matrix N is nilpotent iff $N^\alpha = 0$ for some α. We wish to show that every nilpotent matrix is similar to a matrix of the form:

$$\begin{bmatrix} N_1 & & & \\ & N_2 & & \\ & & \ddots & \\ & & & N_s \end{bmatrix}$$

where each N_i is a square matrix of the form

$$\begin{bmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ & & & 1 & 0 \end{bmatrix}$$

We say two matrices are similar just in case they a have the same national canonical form. So suppose A is a nilpotent matrix. Therefore,

$$
\begin{aligned}
& A^{\alpha} = 0 \\
\Longrightarrow & \underbrace{A \cdot A \cdot A \cdot \ldots \cdot A}_{\alpha} = 0 \\
\Longrightarrow & \underbrace{(A-0I)\cdot(A-0I)\cdot(A-0I)\cdot \ldots \cdot(A-0I) = 0}_{\alpha} = 0 \\
\Longrightarrow & A\text{is a root for the polynomial}\underbrace{(x-0)\cdot(x-0)\cdot(x-0)\cdot \ldots \cdot(x-0)}_{\alpha} \\
\Longrightarrow & \text{A is a root for the polynomial}\underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{\alpha} \\
\Longrightarrow & x^{\alpha} \text{ is the minimal polynomial for A}
\end{aligned}
$$

This minimal polynomial will yield the following $\alpha \times \alpha$ companion matrix:

$$
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
 & 1 & \ddots & & \\
 & & \ddots & 0 & \\
 & & & 1 & 0
\end{bmatrix}
$$

Furthermore, any other invariant factor of A must divide x^{α}, so it must be of the form x^{β_i}, with $\beta_1 \mid \beta_2 \mid \ldots \mid \beta_n \mid \alpha$. Each of these invariant factors will give a $\beta_i \times \beta_i$ matrix of the form:

$$
\begin{bmatrix}
0 & & & & \\
1 & 0 & & & \\
 & 1 & \ddots & & \\
 & & \ddots & 0 & \\
 & & & 1 & 0
\end{bmatrix}
$$

Now, using these companion matrices to construct the rational canonical form for A we will get a matrix of the form:

$$
\begin{bmatrix}
M_1 & & & \\
 & M_2 & & \\
 & & \ddots & \\
 & & & M_t
\end{bmatrix}
$$

Where the M_i's are the square companion matrices as described above. Clearly this is similar to the desired matrix.

4. Suppose R is a P.I.D., A and B are finitely generated R-modules, then A and B are isomorphic to the following:

$$A \cong R^a \oplus \frac{R}{n_1} \oplus \frac{R}{n_2} \oplus \ldots \oplus \frac{R}{n_s} \qquad \text{for } a \geq 0 \text{ and all } n_i \text{ non-zero, non-units satisfying } n_i \mid n_{i+1}$$

$$B \cong R^b \oplus \frac{R}{m_1} \oplus \frac{R}{m_2} \oplus \ldots \oplus \frac{R}{m_t} \qquad \text{for } b \geq 0 \text{ and all } m_i \text{ non-zero, non-units satisfying } m_i \mid m_{i+1}$$

a and b are the ranks of A and B respectively, and the m_i's and n_i's are the respective invariant factors. Two finitely generated R-modules are isomorphic just in case they have the same free rank and list of invariant factors. Suppose $A \oplus A \cong B \oplus B$. This would mean the ranks and list of invariant factors of $A \oplus A$ and $B \oplus B$ are equivalent. We know these ranks to be $2a$ and $2b$ respectively, and clearly if $2a = 2b$ then $a = b$, therefore we know A and B have the same rank. We also know the respective invariant factors of these modules are $\{n_1, n_1, n_2, n_2, ..., n_s, n_s\}$ and $\{m_1, m_1, m_2, m_2, ..., m_t, m_t\}$. Since $A \oplus A \cong B \oplus B$, we know

$$\{n_1, n_1, n_2, n_2, ..., n_s, n_s\} = \{m_1, m_1, m_2, m_2, ..., m_t, m_t\}$$

meaning for any n_i in the first list, there is exactly one corresponding m_j in the second list. If we remove all duplicate copies in the first list and all corresponding values in the second list, leaving $\{n_1, n_2, ..., n_s\}$ and $\{m_1, m_2, ..., m_t\}$ we are left with precisely the invariant factors of A and B. Therefore A and B have the same rank and list of invariant factors, so we may conclude $A \cong B$.

III. Fields

1. a. To find the Galois group over $\mathbb{Q}$ of the polynomial, $x^4 - 25$ we must first find the roots of the polynomial. The roots to this polynomial will be the complex fourth roots of 25.

$$\begin{aligned} w_0 &= \sqrt{5}[cos(0) + isin(0)] = \sqrt{5} \\ w_1 &= \sqrt{5}[cos(\frac{2\pi}{4}) + isin(\frac{2\pi}{4})] = -\sqrt{5} \\ w_2 &= \sqrt{5}[cos(\pi) + isin(\pi)] = i\sqrt{5} \\ w_3 &= \sqrt{5}[cos(\frac{3\pi}{2}) + isin(\frac{3\pi}{2})] = -i\sqrt{5} \end{aligned}$$

So the roots of this polynomial are

$$\sqrt{5}, -\sqrt{5}, i\sqrt{5}, -i\sqrt{5}$$

Hence, the splitting field for this polynomial is $\mathbb{Q}(i, \sqrt{5})$. $x^4 - 25$ is a separable polynomial over $\mathbb{Q}(i, \sqrt{5})$ since it has no repeated roots, therefore the extension $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}$ is Galois. This means the size of the Galois group will be equivalent to the degree of the extension.

$$\begin{aligned} [\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] &= [\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(\sqrt{5})] \cdot [\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] \\ &= 2 \cdot 2 \\ &= 4 \end{aligned}$$

This is because the minimal polynomial are $x^2 + 1$ and $x^2 - 5$ respectively. The automorphisms in the Galois group will be determined by where they send the roots of the minimal polynomials, so they will be generated by the following two automorphisms

$$\sigma = \begin{cases} \sqrt{5} & \longmapsto -\sqrt{5} \\ i & \longmapsto i \end{cases}$$

$$\tau = \begin{cases} \sqrt{5} & \longmapsto \sqrt{5} \\ i & \longmapsto -i \end{cases}$$

The order of each of these automorphism is 2, and together they generate another order 2 automorphism:

$$\tau\sigma = \begin{cases} \sqrt{5} & \longmapsto -\sqrt{5} \\ i & \longmapsto -i \end{cases}$$

Thus, $Gal(\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$. This group will have two subgroups, $\langle\sigma\rangle$ and $\langle\tau\rangle$, each of index 2 in the Galois Group. The corresponding fixed fields for these subgroups will be $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5})$ respectively.

b. We wish to find the Galois group for $x^3 - x + 1$ over $\mathbb{Q}$. The derivative of this polynomial is $3x^2 - 1$, which has roots $\frac{1}{\sqrt{3}}$ and $-\frac{1}{\sqrt{3}}$. However,

$$\frac{1}{\sqrt{3}}^3 - \frac{1}{\sqrt{3}} + 1 = \frac{1 - 3 + 3\sqrt{3}}{3\sqrt{3}} \geq 0$$

and

$$-\frac{1}{\sqrt{3}}^3 + \frac{1}{\sqrt{3}} + 1 = \frac{-1 + 3 + 3\sqrt{3}}{3\sqrt{3}} \geq 0$$

which means that this polynomial has precisely two non-real roots. Furthermore, by the Eisenstein criterion, we know that this polynomial is irreducible. That is, only ± 1 divide the constant term of the polynomial, but ± 1 is not a root of the polynomial. Therefore, we conclude that the Galois group of $x^3 - x + 1$ is isomorphic to the Symmetric group, S_3.

2. a. E is a splitting field for the polynomial $g(x)$ over F if $g(x)$ factors completely into linear factors in $E[x]$, but not in any proper subfield of F containing K.

b. Suppose $g(x) \in F[x]$, and $deg(g(x)) = n$. Suppose α_1 is a root of $g(x)$. Then, $F(\alpha_1) = F_1$ is an extension of at most n over F, since the minimal polynomial over F for which α_1 is a root must be either $g(x)$ itself, or something of degree smaller than $g(x)$. Therefore, $[F_1 : F] = m_1 \leq n$. Now examine another root, α_2 of $g(x)$, and let $F(\alpha_2) = F_2$. Over F_1, we know

$$g(x) = (x^{m_1} - \alpha_1) \cdot f(x)$$

and α_2 is a root for $f(x)$. Again, we know $F(\alpha_2) = F_2$ is an extension of at most $n - m_1$ over F, since the minimal polynomial over F_1 for which α_2 is a root is of degree less than or equal to the degree of $f(x)$. Therefore, $[F_2 : F_1] = n - m_1 \leq n - 1$. This same argument can be repeated for every root of $g(x)$, and once we've adjoined every root to F, we get E. But now we may compute,

$$\begin{aligned}
[E : F] &= [E : F_q] \cdot \ldots \cdot [F_2 : F_1] \cdot [F_1 : F] \\
&\leq (n - m_q) \cdot \ldots \cdot (n - m_1) \cdot (n) \\
&\leq n!
\end{aligned}$$

3. a. In order to compute the Galois group of $x^4 - 4$ we must first compute the roots of the polynomial.

$$\begin{aligned}
w_0 &= \sqrt{2}[\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}] = \sqrt{2}[\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}] = 1 + i \\
w_1 &= \sqrt{2}[\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}] = \sqrt{2}[-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}] = -1 + i \\
w_2 &= \sqrt{2}[\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}] = \sqrt{2}[-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}] = -1 - i \\
w_3 &= \sqrt{2}[\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}] = \sqrt{2}[\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}] = 1 - i
\end{aligned}$$

The roots of this polynomial are $\pm 1 \pm i$, and so the splitting field for the polynomial is $\mathbb{Q}(i)$. Since the polynomial has no repeated roots, we know that is is separable over $\mathbb{Q}$, therefore $\mathbb{Q}(i)$ is Galois over $\mathbb{Q}$. This implies

$$\mid Gal(\mathbb{Q}(i)/\mathbb{Q}) \mid = [\mathbb{Q}(i) : \mathbb{Q}] = 2$$

since $x^2 + 1$ is the minimal polynomial over $\mathbb{Q}$ for which i is a root. Any automorphism in this Galois group must take roots to roots, so our only choice is

$$\sigma : i \longrightarrow -i$$

which is an automorphism of order 2. Therefore

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$$

b. We wish to find the Galois group of $x^3 + x^2 - 2x - 1$. Suppose that r is a root of this polynomial, so $r^3 + r^2 - 2r - 1 = 0$. This means that over its splitting field, this polynomial contains the linear factor, $(x - r)$. Using long division of polynomials, it is possible to divide out by this factor and see that

$$x^3 + x^2 - 2x - 1 = (x - r)(x^2 + (1 + r)x + (-2 + r + r^2))$$

and we may now show that $r^2 - 2$ is a root for this polynomial.

$$\begin{aligned}
&((r^2 - 2)^2 + (1 + (r^2 - 2))x + (-2 + (r^2 - 2) + (r^2 - 2)^2)) \\
=&r^4 - 4r^2 + 4 + r^2 + r^3 - 2r - 2 - 2 + r + r^2 \\
=&r^4 + r^3 - 2r^2 - r \\
=&r(r^3 + r^2 - 2r - 1) \\
=&r(0) \\
=&0
\end{aligned}$$

So now we know this polynomial has roots, r, $r^2 - 2$, and $(r^2 - 2)^2 - 2$. By the Eisenstein Criterion we can see that the polynomial is irreducible, since ± 1 are not roots for the polynomial. Therefore we know that none of the roots are in $\mathbb{Q}$ and hence the polynomial splits into no linear factors over $\mathbb{Q}$. This now tells us that to get the splitting field, we must to adjoin all roots to $\mathbb{Q}$, and

$$[\mathbb{Q}(r, r^2-2, (r^2-2)^2-2) : \mathbb{Q}] = 3$$

since adjoining r yields all other roots, and clearly x^3+x^2-2x-1 is the minimal polynomial for which r is a root. Now we know that the size of the Galois group is precisely three, which means there is only one possibility for the Galois group, namely

$$Gal(\mathbb{Q}(r, r^2-2, (r^2-2)^2-2)/\mathbb{Q}) \cong \mathbb{Z}_3$$

4. First we will show that every finite group G, of order n, is isomorphic to a subgroup of the symmetric groupS_n. To show this, suppose $H \leq G$ and $H = 1$. The set of coset of H in G will just be the group G itself. So let's examine the permutation representation generated by G acting on itself by left multiplication. We define the following for any $g \in G$

$$\begin{aligned} \sigma_g :& G \longrightarrow G \\ & g' \longrightarrow g \cdot g' \end{aligned}$$

and the associated permutation representation

$$\begin{aligned} \pi_H :& G \longrightarrow S_G \\ & g \longrightarrow \sigma_g \end{aligned}$$

Defined as such, $ker(\pi_H)$ will be the largest normal subgroup of G contained in H, but since $H = 1$, this means $ker(\pi_H) = 1$. Now by the First Isomorphism Theorem for groups we know,

$$G/ker(\pi_H) \cong Im(\pi_H) \leq S_G$$

However, since $ker(\pi_H) = 1$, this actually means $G \leq S_G$.

Now we wish to show that there exist fields $E \supseteq F$ such that $gal(E/F) \cong G$ for a finite group G of order n. Examine the field $\mathbb{Q}(S_1, S_2, ..., S_n)$ where the S_i's are the elementary symmetric polynomials in i variables. Then we define the general polynomial of degree n as

$$g(t) = t^n - S_1t^{n-1} + S_2t^{n-2} - ... + (-1)^n S_n$$

We know the splitting field for this polynomial is $\mathbb{Q}(x_1, x_2, ...x_n)$ and $g(t)$ splits into linear factors over this field. It is a fact, that

$$Gal(\mathbb{Q}(x_1, x_2, ...x_n)/\mathbb{Q}(S_1, S_2, ..., S_n)) \cong S_n$$

for the symmetric group S_n, and we know that G is isomorphic to a subgroup of S_n. Now by the fundamental theory of Galois Theory we may conclude that there is some field F, such that

$$\mathbb{Q}(S_1, S_2, ..., S_n) \subseteq F \subseteq \mathbb{Q}(x_1, x_2, ...x_n)$$

such that

$$Gal(\mathbb{Q}(x_1, x_2, ...x_n)/F) \cong G$$

and so we are done.

ALGEBRA QUALIFYING EXAM, SUMMER 2007

There are three pages to the exam, one each on the topics of groups, rings, and fields.

1. Groups

Do problem 1 in this section, and do *two* of problems 2 through 4. Please indicate clearly which problem you choose to omit.

(1) (a) State the Sylow theorems.
(b) Show that in a group of order 105, either the 5-Sylow or the 7-Sylow subgroup is normal.
(c) Show that a group of order 105 has a normal subgroup of order 35.
(d) Show that in a group of order 105, both the 5-Sylow and the 7 Sylow subgroups are normal.

(2) Let $n > 1$ be an integer. Show that the automorphism group of the cyclic group of order n is isomorphic to the multiplicative group of units mod n.

(3) Let G be a group with center $Z(G)$. Show that if $G/Z(G)$ is cyclic, then G is abelian.

(4) Let x,y be 3-cycles in S_5, x not equal to y or y^{-1}.
(a) If there is some element of $\{1, 2, 3, 4, 5\}$ fixed by both x and y, show that $< x, y >$ is isomorphic to A_4.
(b) If there is no such element fixed by both, show that $< x, y >= A_5$.

2. Rings

Do problem 1 in this section and do *two* of problems 2 through 4. Please indicate clearly which problem you choose to omit.

(1) Give an example of each of the following. (You don't need to justify your answers.)

(a) A maximal ideal of $\mathbf{Z}[x]$.
(b) A ring R and an ideal I of R that is prime but not maximal.
(c) A ring R and a module M over R which is torsion free but isn't free.
(d) A unique factorization domain which isn't a PID.
(e) A ring which isn't Noetherian.

(2) Show that the characteristic of an integral domain must be either zero or a prime.

(3) Let O be the ring of integers of $\mathbf{Q}(\sqrt{2})$. Show that O is a Euclidean domain with respect to the usual field norm $N(a+b\sqrt{2}) = a^2 - 2b^2$.

(4) (a) List all abelian groups of size 90.
(b) List all $\mathbf{R}[x]$ modules M such that $\dim_{\mathbf{R}} M = 4$ and M is annihilated by $x^4 - 1$.

3. Fields

Do problem 1 in this section and do *three* of problems 2 though 5. Please indicate clearly which problem you choose to omit.

(1) Let K be the splitting field of $x^3 - 7$ over $\mathbf{Q}$.
  (a) Find the Galois group of K over $\mathbf{Q}$.
  (b) Find all of the subfields of K.
  (c) Which of the subfields you found above are Galois over $\mathbf{Q}$?

(2) Let L be the splitting field of $x^5 - 3$ over $\mathbf{Q}$.
  (a) Let ζ_5 be a primitive 5th root of unity. Prove that $\mathbf{Q}(\zeta_5) \subset L$.
  (b) What is the Galois group of L over $\mathbf{Q}(\zeta_5)$?
  (c) What is the dimension of L over $\mathbf{Q}$?

(3) (a) Suppose that K is a Galois extension of $\mathbf{Q}$ of dimension 2^n for some positive integer n. Prove that every element of K is constructible.
  (b) Suppose $f(x) \in \mathbf{Q}[x]$ is an irreducible quartic such that the splitting field of $f(x)$ over $\mathbf{Q}$ has dimension 24. Suppose α is a root of $f(x)$. Prove that α is not constructible.

(4) (a) Let F be a field, and let K, L be finite dimensional extensions of F. Suppose $[K : F]$ and $[L : F]$ are relatively prime. Prove that $[KL : F] = [K : F][L : F]$. Here KL is the compositum of K and L.
  (b) Give an example of fields F, K, L such that $K \cap L = F$ and $[KL : F] < [K : F][L : F]$.

(5) (a) Show that a finite field must have exactly p^n elements for some prime p and some positive integer n.
  (b) List all the subfields of the field of size 3^{12}.
  (c) Give an example of an infinite field of characteristic 3.

Algebra Qualifying Exam of July 12, 2006

The exam has three sections. In each section, please answer both starred problems and one of the two other problems. Note that some of the starred problems have several parts.

Section I. Groups.

*1. (a) State the class equation for finite groups.

(b) Use the class equation to show that if a finite group G has order p^k for some prime p and $k \geq 1$, then G has a nontrivial center.

*2. Let G be a group of order $p^k m$, where p is a prime not dividing m.

(a) What is a Sylow p-subgroup of G?

(b) State Sylow's theorem, including information about the number of Sylow p-subgroups of G and about relationships between them.

(c) Show that there are no simple groups of order 132.

3. Let G be a finite group of order n and let p be the smallest prime dividing n. Show that any subgroup of G of index p is normal in G.

4. If p is a prime, k is a positive integer and G is a group of order p^k, show that for each positive integer $l \leq k$, G has a normal subgroup of order p^l.

Section II. Fields.

*5. Let K and F be fields, with K a finite-dimensional algebraic extension of F.

(a) Give the definition of "K is a Galois extension of F."

(b) State the Fundamental Theorem of Galois Theory.

*6. Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$, the field of rational numbers. What is $[K : \mathbb{Q}]$? Describe the Galois group $G = Gal(K/\mathbb{Q})$: either find generators of the group and indicate relations among those generators which determine its multiplication table, or identify a familiar group to which G is isomorphic. Find all the subgroups of G and their orders, and indicate the corresponding subfields of K.

7.(a) Describe the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, where p is a prime and $n \geq 1$.

(b) Find fields K and F such that K is a splitting field over F, but K is *NOT* separable over F.

8. Show that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Section III. Rings and modules.

*9. (a) State the structure theorem for finitely generated Abelian groups. (You may give either the elementary divisor decomposition or the invariant factor decomposition.)

(b) Up to isomorphism, what are the Abelian groups of order $300 (= 2^2 \cdot 3 \cdot 5^2)$? You should give a list of pairwise non-isomorphic Abelian groups, of order 300, such that every Abelian group of order 300 is isomorphic to a group on the list.

*10.(a) What is a principal ideal domain?

(b) Consider the four rings $\mathbb{Q}[x], \mathbb{Q}[x]/(x^2 - 2), \mathbb{Q}[x]/(x^2 - 4)$, and $\mathbb{Q}[x, y]$. Which of these rings are principal ideal domains, and which are not? Explain.

11. Give an example of an integral domain R, a free R-module M, and an R-submodule N of M such that N is not a free R-module.

12. Find the rational canonical form over $\mathbb{Q}$ of the following matrix:

$$\begin{pmatrix} 3 & -1 & 10 \\ 0 & 2 & 5 \\ 0 & 0 & 3 \end{pmatrix}.$$

Algebra Preliminary Examination

Summer 2005

Do as much as you can. You should try to say something about every problem.

1. (a) State Sylow's theorems.

   (b) Classify up to isomorphism the groups of order 35.

   (c) Show that there are no simple groups of order 24.

2. (a) State the structure theorem for finite Abelian groups.

   (b) Up to isomorphism, what are the Abelian groups of order 360? You should give a list of pairwise non-isomorphic Abelian groups of order 360, such that every Abelian group of order 360 is isomorphic to a group on the list.

3. (a) State the definition of a principal ideal domain.

   (b) Let $\mathbb{Z}$ be the ring of integers. Is $\mathbb{Z}[x]$ a principal ideal domain? Either prove that it is, or present an example showing that it is not.

4. Let K be the splitting field of $(x^3 - 2)(x^2 - 3)$ over $\mathbb{Q}$ and G be the Galois group of $K/\mathbb{Q}$.

   (a) For each prime divisor p of $|G|$, decide whether G has a normal Sylow p-subgroup.

   (b) Show that there are subgroups G_1 and G_2 of G such that

      i. $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright G_3 = \{1\}$;

      ii. G_i/G_{i+1} is a cyclic group of prime order for $i = 0, 1, 2$.

   Determine also the subfields of K corresponding to the G_is under the Galois correspondence.

5. Let F be a field of 81 elements. For each of the following polynomials, determine the number of roots that lie in F: $x^{80} - 1, x^{81} - 1, x^{88} - 1$.

6. Two $n \times n$ matrices A and B over a field F are said to be similar if there exists an $n \times n$ invertible matrix T over F such that $TAT^{-1} = B$. Exhibit three 3×3 matrices over $\mathbb{Q}$ no two of which are similar such that -2 is the only rational eigenvalue of each of the matrices. For each of these three matrices, determine its elementary divisors, minimal polynomial and characteristic polynomial.

ALGEBRA PRELIMINARY EXAM - 2004

There are three sections, corresponding roughly to "groups", "rings" and "fields". You may omit one problem in each section, but you must do all of the problems numbered "1". Please write OMIT on the problem you choose.

1. Groups

(1) (a) Prove that all groups of size 15 are solvable.

(b) Prove there are no simple groups of size 36.

(2) Prove that any group of size 15 is cyclic.

(3) List all isomorphism classes of groups of size 72.

(4) Let G be a group and let p be the smallest prime divisor of $|G|$. Suppose that H is a subgroup of G of index p. Prove that H is normal.

2. Rings

(1) Give an example of each of the following. You do not need to justify your answers.
  (a) A Euclidean domain.

  (b) A Unique Factorization Domain that is not a PID.

  (c) An integral domain that is not a Unique Factorization Domain.

(2) (a) Find the rational canonical form of $\begin{pmatrix} 2 & 3 \\ 7 & 1 \end{pmatrix}$.

  (b) Find all possible rational canonical forms for 4-by-4 matrices over the complex numbers whose characteristic polynomial is $(x^2+1)(x+1)^2$.

(3) A commutative ring R is called a *local ring* if it has a unique maximal ideal. Prove that if R is a local ring with maximal ideal M then an element $a \in R$ is a unit if and only if $a \notin M$. Conversely, prove that if R is a commutative ring in which the set of nonunits forms an ideal, then R is a local ring.

3. Fields

(1) This question will ask you to describe the splitting field K of the polynomial $x^4 - 5$ over $\mathbf{Q}$.

(a) What is $[K : \mathbf{Q}]$?

(b) What is the Galois group G of K over $\mathbf{Q}$?

(c) Find all the subgroups of G and describe their fixed fields.

(d) Which of the fixed fields in part c) is Galois over $\mathbf{Q}$?

(2) Given a finite group G, show that there are fields K and F such that K is Galois over F, and G is isomorphic to the Galois group of K over F.

(3) (a) Give an example of an extension of degree 3 over $\mathbf{Q}$ which is *not* Galois over $\mathbf{Q}$.

(b) Suppose K is a Galois extension of $\mathbf{Q}$ with $[K : F] = 105$, and that L is a subfield of K with $[L : \mathbf{Q}] = 3$. Show that L *is* Galois over $\mathbf{Q}$.

(4) (a) Let F be a field of order 5^{20}. List the orders of all the subfields of F.

(b) Does F have more than one subfield of order 25? Explain.

Algebra Preliminary Examination: July 28, 2003

This is a closed book, timed exam. You may not consult any books, notes, homeworks, or other sources. All work should be your own.

Each problem will be weighted equally.

You may begin at 9:00 a.m. and should hand in your exam by 12 noon.

1. Let G be a group of order 84 with 28 Sylow 3-subgroups.

   (a) Find the number of Sylow 7-subgroups of G.

   (b) Let Q be a Sylow 3-subgroup of G. Let $N_G(Q)$ be the normalizer of Q in G, and $Z_G(Q)$ be the centralizer of Q in G. Show that $N_G(Q) = Z_G(Q) = Q$.

2. Let D_8 be the dihedral group with 8 elements. Show that every Sylow 2-subgroup of S_8 contains a normal subgroup that is isomorphic to $D_8 \times D_8$.

3. (a) Let R be the ring of all polynomials in $\mathbf{Q}[x]$ having no x-term. Show that x^5 and x^6 have no gcd in R.

(b) If S is an Euclidean domain and T is a subring of S, is it true that T is an Euclidean domain? Justify your answer.

4. Let F be a field of order 1024.

(a) Find the prime field of F.

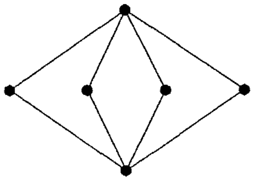
(b) Let K be a subfield of F. Find all possible orders for K.

5. Find the Galois group of $x^4 + x^3 + x^2 + x + 1$

(a) over $\mathbf{Q}$.

(b) over $\mathbf{F}_5$.

6. Let E be a splitting field of $g(x) \in \mathbf{Q}[x]$ over $\mathbf{Q}$. Suppose that the lattice of intermediate fields between E and $\mathbf{Q}$ is isomorphic to



Which of the following groups could be $Gal(E/\mathbf{Q})$?
Justify your answers.

(a) $\mathbf{Z}_2 \times \mathbf{Z}_2$ under $+$.

(b) $\mathbf{Z}_6$ under $+$.

(c) the dihedral group with 6 elements.

(d) S_3.

(e) $\mathbf{Z}_3 \times \mathbf{Z}_3$ under $+$.

7. Prove that if F is a field and $g(x) \in F[x]$ has a root $\alpha \in F$, then its Galois group is the same as the Galois group of $g(x)/(x - \alpha)$.

8. (a) How many abelian groups of order 720 are there?

(b) Let L, M, N be finitely generated $\mathbf{Z}$-modules, such that $L \oplus M \cong L \oplus N$. Prove that $M \cong N$.

9. (a) Given a group G, state the criteria that make G a solvable group. Use your definition to prove that S_4 is solvable.

(b) Let $g(x) \in \mathbf{Q}[x]$ have degree 4. Prove or disprove: $g(x)$ is not solvable by radicals.

(c) Let $g(x) \in \mathbf{Q}[x]$ have degree 5. Prove or disprove: $g(x)$ is not solvable by radicals.