Practice problems for first midterm, Spring '98

midterm to be held Wednesday, February 25, 1998, in class

Dave Bayer, Modern Algebra

All rings are assumed to be commutative with identity, as in our text.

[1] Prove that if a ring R has no ideals other than (0) and (1), then R is a field.

[2] Prove that if an integral domain R has only finitely many elements, then R is a field.

[3] Consider the ideal $I = (5, x^2) \subset \mathbb{Z}[x]$.

(a) Describe the ideal I in words. How would you tell at a glance if a given polynomial $f(x) \in \mathbb{Z}[x]$ belongs to I?

(b) List the elements of the quotient ring $R = \mathbb{Z}[x]/I$, and describe the multiplication rule for R.

[4] Repeat problem 3 for $I = (x^3, xy, y^3) \subset \mathbb{F}_2[x, y]$, where $\mathbb{F}_2$ is the finite field with two elements.

[5] The ideal $I = (2, 1+3i) \subset \mathbb{Z}[i]$ is principal, where $\mathbb{Z}[i]$ are the Gaussian integers. Find a single generator for I. (Repeat for $I = (3, 1+i)$, and $I = (6, 3+5i)$.)

[6] Let F be a field. The ideal $I = (1 - x^2, 1 - 3x + 3x^2 - x^3) \subset F[x]$ is principal. Find a single generator for I.

[7] Consider the polynomial ring $R = \mathbf{C}[x, y]$, where $\mathbf{C}$ is the field of complex numbers.

(a) What are the maximal ideals of R?

(b) Which maximal ideals contain the ideal $I = (xy) \subset R$?

(c) What are the maximal ideals of the quotient ring R/I?

[8] Let $\mathbf{X} \subset \mathbb{R}^3$ be the union of the x-axis, y-axis, and z-axis in $\mathbb{R}^3$, where $\mathbb{R}$ denotes the real numbers. Define $I \subset \mathbb{R}[x, y, z]$ to be the set of all polynomials $f(x, y, z)$ that vanish on every point of $\mathbf{X}$. That is,

$$I \quad = \quad \{\ f(x,y,z) \in \mathbb{R}[x,y,z] \mid f(a,b,c) = 0 \text{ for every point } (a,b,c) \in X\ \}.$$

(a) Prove that I is an ideal. (Your proof only needs to use the fact that $\mathbf{X}$ is *some* subset of $\mathbb{R}^3$.)

(a) Give a set of generators for I.

[9]

(a) Prove that every positive integer can be uniquely factored into primes, up to the order of the primes.

(b) How do you need to modify this proof so it works for a polynomial ring in one variable over a field?

[10] Let R be a principal ideal domain, and let

$$I_1 \quad \subset \quad I_2 \quad \subset \quad I_3 \quad \subset \quad \cdots \quad \subset \quad I_n \quad \subset \quad \cdots$$

be an infinite ascending chain of ideals in R. Show that this chain *stabilizes*, i.e.

$$I_N \quad = \quad I_{N+1} \quad = \quad I_{N+2} \quad = \quad \cdots$$

for some N.

First midterm

Dave Bayer, Modern Algebra, February 25, 1998

All rings are commutative with identity, as in our text. Recall that an *integral domain* R is a nonzero ring having no zero divisors. In other words, if $ab = 0$ then $a = 0$ or $b = 0$.

[1] Consider the ideal $I = (2, x^3 + x) \subset \mathbb{Z}[x]$.

(a) Describe the ideal I in words, listing enough elements of I to make the pattern clear. How would you tell at a glance if a given polynomial $f(x) \in \mathbb{Z}[x]$ belongs to I?

(b) List representatives for the elements of the quotient ring $R = \mathbb{Z}[x]/I$, and describe the multiplication rule in R for these representatives.

(c) Is R an integral domain?

[2] Let $a = 3 - i$ and $b = 2i$ be elements of the Gaussian integers $\mathbb{Z}[i]$.

(a) Find q_1, $c \in \mathbb{Z}[i]$ so $a = q_1\, b + c$ with $|c| < |b|$.

(b) Now find q_2, $d \in \mathbb{Z}[i]$ so $b = q_2\, c + d$ with $|d| < |c|$.

(c) Express $(a, b) \subset \mathbb{Z}[i]$ as a principal ideal.

[3] Prove that the following two statements are equivalent, for a nonzero ring R and elements a, b, $c \in R$:

(a) R is an integral domain.

(b) We can *cancel* in R: If $ab = ac$ for $a \neq 0$, then $b = c$.

[4] Prove that if an integral domain R has only finitely many elements, then R is a field.

[5] Let $\mathbb{F}_5$ be the finite field with 5 elements. Find a polynomial $f(x)$ in the polynomial ring $\mathbb{F}_5[x]$ such that the quotient ring $\mathbb{F}_5[x]/(f(x))$ is a field with 25 elements.

First Midterm Exam

Modern Algebra, Dave Bayer, February 17, 1999

Name: ______________________________

ID: ____________________ **School:** ____________________

[**1**] (6 pts)	[**2**] (6 pts)	[**3**] (6 pts)	[**4**] (6 pts)	[**5**] (6 pts)	**TOTAL**

Each problem is worth 6 points, for a total of 30 points. Please work only one problem per page, and label all continuations in the spaces provided. Extra pages are available.

[**1**] Consider the ideal $I = (x^3, 2x, 4) \subset \mathbb{Z}[x]$.

(a) List representatives for the elements of the quotient ring $R = \mathbb{Z}[x]/I$, and describe the multiplication rule in R for these representatives.

(b) Is R an integral domain?

 Continued on page: ______

Problem: ______

Continued on page: ______

[2] Prove that if a ring R has no ideals other than (0) and (1), then R is a field.

Continued on page: ______

Problem: ______

Continued on page: ______

[3] Prove that if an integral domain R has only finitely many elements, then R is a field. Prove any lemmas that you use.

Continued on page: ______

Problem: ______

Continued on page: ______

[4] Let $\mathbb{F}_3$ be the finite field with 3 elements. Find a polynomial $f(x)$ in the polynomial ring $\mathbb{F}_3[x]$ such that the quotient ring $\mathbb{F}_3[x]/(f(x))$ is a field with 27 elements.

 Continued on page: ______

Problem: ______

Continued on page: ______

[5] Let $\mathbf{X} \subset \mathbb{R}^2$ be the union of the parabola $y = x^2$ and the point $(0, 1)$. Define $I \subset \mathbb{R}[x, y]$ to be the set of all polynomials $f(x, y)$ that vanish on every point of $\mathbf{X}$. That is,

$$I \quad = \quad \{\ f(x,y) \in \mathbb{R}[x,y] \ \mid\ f(a,b) = 0 \ \text{ for every point } \ (a,b) \in X\ \}.$$

(a) Prove that I is an ideal.
(b) Give a set of generators for I.

Continued on page: ______

Problem: ______

Continued on page: ______

Practice problems for second midterm

midterm to be held Wednesday, April 8, in class

Dave Bayer, Modern Algebra

We will have a problem session in preparation for this midterm:

- Monday, April 6, 8:00pm - 10:00pm, 507 Mathematics

[**1**] Prove the *Eisenstein criterion* for irreducibility: Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let p be a prime. If p doesn't divide a_n, p does divide $a_{n-1}, \ldots, a_0$, but p^2 doesn't divide a_0, then $f(x)$ is irreducible as a polynomial in $\mathbb{Q}[x]$.

(a) First, what does $f(x)$ look like mod p?

(b) Now, suppose that there is a nontrivial factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. What do $g(x)$ and $h(x)$ look like mod p? What would this imply about a_0?

[**2**] Prove that $f(x) = x^{p-1} + \ldots + x + 1$ is irreducible when p is prime:

(a) Show that $(x-1)f(x) = x^p - 1$.

(b) Now set $x = y + 1$, so $(x-1)f(x) = yf(y+1) = (y+1)^p - 1$. Study the binomial coefficients in the expansion of $(y+1)^p$, and apply the Eisenstein criterion to $f(y+1)$.

[**3**] Let p be a prime so $p-1$ is not a power of 2. Prove that the p-gon is not constructible:

(a) Let $\theta = 2\pi/p$, and let $z = \cos\theta + i\sin\theta$. Explain why, if $\cos\theta$ and $\sin\theta$ are constructible, then the degree of z over $\mathbb{Q}$ is a power of 2.

(b) Show that z is a root of $x^p - 1$ but not $x - 1$, so z is a root of the irreducible polynomial $f(x) = x^{p-1} + \ldots + x + 1$. Thus, the degree of z over $\mathbb{Q}$ is not a power of 2.

[**4**] Show that the set of constuctible numbers form a field.

[**5**] Prove that the cube root of 5 is not a constructible number.

[**6**] Show *algebraically* that it is possible to construct an angle of 30°.

[**7**] Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 8 & 8 \end{bmatrix}$. Reduce A to diagonal form, using row and column operations.

[8] Let G be the *Abelian* group $G = \langle\, a, b, c \mid a^2b^2c^2 = a^2b^2 = a^2c^2 = 1 \,\rangle$. Express G as a product of free and cyclic groups.

[9] Let $R = k[x_1, \dots, x_n]$ be the polynomial ring in $x_1, \dots, x_n$ over a field k, and let $f_1, \dots, f_m$ be m polynomials in R. Let R^m be the free R-module $R^m = \{\, (g_1, \dots, g_m) \mid g_i \in R \text{ for } 1 \le i \le m \,\}$. Let $M \subset R^m$ be the subset of *syzygies* $M = \{\, (g_1, \dots, g_m) \mid g_1 f_1 + \ldots + g_m f_m = 0 \,\}$.

(a) Show that M is an R-module.

(b) Let $R = \mathbb{Q}[x, y]$, $m = 3$, and $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$. Find a set of generators for $M \subset R^3$.

[10] Suppose that the complex number α belongs to an extension K of $\mathbb{Q}$ of degree 9, and an extension L of $\mathbb{Q}$ of degree 12, but not to $\mathbb{Q}$ itself. What is the degree of α over $\mathbb{Q}$?

[11] Show that every element of $\mathbb{F}_{25}$ is a root of the polynomial $x^{25} - x$.

[12] Give a presentation of $\mathbb{F}_9$ of the form $\mathbb{F}_3[x]/(f(x))$. In terms of this presentation, find a generator α of the multiplicative group $\mathbb{F}_9^*$, i.e. an element of multiplicative order $9 - 1 = 8$.

Practice Problems for Second Midterm Exam

Modern Algebra, Dave Bayer, March 29, 1999

This first set of problems are collected from various materials already posted on the web.

[**1**] Working in the Gaussian integers $\mathbb{Z}[i]$, factor 2 into primes.

[**2**] Let $a = 3 - i$ and $b = 2i$ be elements of the Gaussian integers $\mathbb{Z}[i]$.
(a) Find $q_1,\, c \in \mathbb{Z}[i]$ so $a = q_1\, b + c$ with $|c| < |b|$.
(b) Now find $q_2,\, d \in \mathbb{Z}[i]$ so $b = q_2\, c + d$ with $|d| < |c|$.
(c) Express $(a, b) \subset \mathbb{Z}[i]$ as a principal ideal.

[**3**] The ideal $I = (2, 1+3i) \subset \mathbb{Z}[i]$ is principal, where $\mathbb{Z}[i]$ are the Gaussian integers. Find a single generator for I. (Repeat for $I = (3, 1+i)$, and $I = (6, 3+5i)$.)

[**4**]
(a) Prove that every positive integer can be uniquely factored into primes, up to the order of the primes.
(b) How do you need to modify this proof so it works for a polynomial ring in one variable over a field?

[**5**] Let R be a principal ideal domain, and let

$$I_1 \quad\subset\quad I_2 \quad\subset\quad I_3 \quad\subset\quad \cdots \quad\subset\quad I_n \quad\subset\quad \cdots$$

be an infinite ascending chain of ideals in R. Show that this chain *stabilizes*, i.e.

$$I_N \quad=\quad I_{N+1} \quad=\quad I_{N+2} \quad=\quad \cdots$$

for some N.

[**6**] Prove the *Eisenstein criterion* for irreducibility: Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let p be a prime. If p doesn't divide a_n, p does divide $a_{n-1}, \ldots, a_0$, but p^2 doesn't divide a_0, then $f(x)$ is irreducible as a polynomial in $\mathbf{Q}[x]$.
(a) First, what does $f(x)$ look like mod p?
(b) Now, suppose that there is a nontrivial factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$. What do $g(x)$ and $h(x)$ look like mod p? What would this imply about a_0?

[**7**] Prove that $f(x) = x^{p-1} + \ldots + x + 1$ is irreducible when p is prime:
(a) Show that $(x-1)f(x) = x^p - 1$.
(b) Now set $x = y + 1$, so $(x-1)f(x) = yf(y+1) = (y+1)^p - 1$. Study the binomial coefficients in the expansion of $(y+1)^p$, and apply the Eisenstein criterion to $f(y+1)$.

[**8**] Show that the following polynomials in $\mathbb{Z}[x]$ cannot be factored:

(a) $x^3 + 6x^2 + 9x + 12$
(b) $x^2 + x + 6$

[9] Let $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 8 & 8 & 8 \end{bmatrix}$. Reduce A to diagonal form, using row and column operations.

[10] Let G be the *Abelian* group $G = \langle\, a, b, c \mid a^2b^2c^2 = a^2b^2 = a^2c^2 = 1 \,\rangle$. Express G as a product of free and cyclic groups.

[11] Let G be the *Abelian* group $G = \langle\, a, b, c \mid b^2c^2 = a^6b^2c^2 = a^6b^4c^4 = 1 \,\rangle$. Express G as a product of free and cyclic groups.

[12] Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring in $x_1, \ldots, x_n$ over a field k, and let $f_1, \ldots, f_m$ be m polynomials in R. Let R^m be the free R-module $R^m = \{\, (g_1, \ldots, g_m) \mid g_i \in R \text{ for } 1 \leq i \leq m \,\}$. Let $M \subset R^m$ be the subset of *syzygies* $M = \{\, (g_1, \ldots, g_m) \mid g_1 f_1 + \ldots + g_m f_m = 0 \,\}$.
(a) Show that M is an R-module.
(b) Let $R = \mathbf{Q}[x, y]$, $m = 3$, and $f_1 = x^2$, $f_2 = xy$, $f_3 = y^2$. Find a set of generators for $M \subset R^3$.

[13] Show that every element of $\mathbb{F}_{25}$ is a root of the polynomial $x^{25} - x$.

[14] What is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$?

This second set of problems are new, but are predicted by our assignments.

[15] Let F be a field, and let $f(x)$ be a polynomial of degree n with coefficients in F. Prove that $f(x)$ has at most n roots in F.

[16] Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ be an integer polynomial, and let p be a prime integer which doesn't divide a_n. Prove that if the remainder $\overline{f(x)}$ of $f(x)$ mod p is irreducible, then $f(x)$ is irreducible.

[17] Let F be a field of characteristic $\neq 2$, and let K be an extension of F of degree 2. Prove that K can be obtained by adjoining a square root: $K = F(\delta)$, where $\delta^2 = D$ is an element of F.

[18] Let $F \subset K$ be a finite extension of fields. Define the degree symbol $[K : F]$.

[19] Let $F \subset K \subset L$ be a tower of finite field extensions. Prove that $[L : F] = [L : K][K : F]$.

[20] Consider the module $M = F[x]/((x-2)^3)$ over the ring $R = F[x]$ for a field F.
(a) What is the dimension of M as an F-vector space?
(b) Find a basis for M as an F-vector space, for which the matrix representing multiplication by x is in Jordan canonical form.

Second midterm

Dave Bayer, Modern Algebra, April 8, 1998

[1] Prove the *Eisenstein criterion* for irreducibility: Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let p be a prime. If p doesn't divide a_n, p does divide $a_{n-1}, \ldots, a_0$, but p^2 doesn't divide a_0, then $f(x)$ is irreducible as a polynomial in $\mathbb{Q}[x]$.

[2] Show that the following polynomials in $\mathbb{Z}[x]$ cannot be factored:
(a) $x^3 + 6x^2 + 9x + 12$
(b) $x^2 + x + 6$

[3] Decide, with proof, whether or not each of the following angles can be constructed.
(a) $\theta = 2\pi/6$
(b) $\theta = 2\pi/7$
(c) $\theta = 2\pi/8$

[4] Let G be the *Abelian* group $G = \langle\, a, b, c \mid b^2c^2 = a^6b^2c^2 = a^6b^4c^4 = 1 \,\rangle$. Express G as a product of free and cyclic groups.

[5] Give a presentation of the finite field with eight elements $\mathbb{F}_8$, of the form $\mathbb{F}_2[x]/(f(x))$. In terms of this presentation, find a generator α of the multiplicative group $\mathbb{F}_8^*$.

Second Midterm Exam

Modern Algebra, Dave Bayer, March 31, 1999

Name: ____________________

ID: ____________________ **School:** ____________________

[**1**] (6 pts)	[**2**] (6 pts)	[**3**] (6 pts)	[**4**] (6 pts)	[**5**] (6 pts)	**TOTAL**

Each problem is worth 6 points, for a total of 30 points. Please work only one problem per page, and label all continuations in the spaces provided. Extra pages are available. Check your work, where possible.

[**1**] Let G be the abelian group $G = \langle\, a, b, c \mid a^7bc^2 = ab^4c^5 = abc^2 = 1 \,\rangle$. Express G as a product of free and cyclic groups.

 Continued on page: ______

Problem: ______

Continued on page: ______

[**2**] What is the minimal polynomial of $\alpha = \sqrt{-1} + \sqrt{2}$ over $\mathbf{Q}$?

 Continued on page: ______

Problem: ______

Continued on page: ______

[3] Consider the module $M = F[x]/(x^3 + 3x^2 + 3x + 1)$ over the ring $R = F[x]$ for a field F.

(a) What is the dimension of M as an F-vector space?

(b) Find a basis for M as an F-vector space, for which the matrix representing multiplication by x is in Jordan canonical form. Give this matrix.

 Continued on page: ______

Problem: ______

Continued on page: ______

[4] Prove the *Eisenstein criterion* for irreducibility: Let $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, and let p be a prime. If p doesn't divide a_n, p does divide $a_{n-1}, \ldots, a_0$, but p^2 doesn't divide a_0, then $f(x)$ is irreducible as a polynomial in $\mathbf{Q}[x]$.

 Continued on page: ______

Problem: ______

Continued on page: ______

[5] Let R be a principal ideal domain, and let

$$I_1 \quad \subset \quad I_2 \quad \subset \quad I_3 \quad \subset \quad \cdots \quad \subset \quad I_n \quad \subset \quad \cdots$$

be an infinite ascending chain of ideals in R. Show that this chain *stabilizes*, i.e.

$$I_N \quad = \quad I_{N+1} \quad = \quad I_{N+2} \quad = \quad \cdots$$

for some N.

 Continued on page: ______

Problem: ______

Continued on page: ______

Practice problems for final exam

Final to be held Wednesday, May 13, 1:10pm - 4:00pm

We will have a problem session in preparation for this final:

- Monday, May 11, 8:00pm - 10:00pm, 507 Mathematics

[**1**] Let $f(x,y,z) = x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2$. Express $f(x)$ as a polynomial $g(\sigma_1, \sigma_2, \sigma_3)$ where σ_1, σ_2, σ_3 are the elementary symmetric functions

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + xz + yz, \quad \sigma_3 = xyz.$$

[**2**] Let $f(x) = x^2 + ax + b$ have roots α_1 and α_2, where

$$\alpha_1 + \alpha_2 = c, \qquad \alpha_1^2 + \alpha_2^2 = d.$$

Express a and b in terms of c and d.

Recall that the discriminant of $f(x) = x^2 + bx + c$ is $D = b^2 - 4c$, and that the discriminant of $f(x) = x^3 + px + q$ is $D = -4p^3 - 27q^2$.

[**3**] Let $f(x) = x^3 - 2$.

(a) What is the degree of the splitting field K of f over $\mathbb{Q}$?

(b) What is the Galois group $G = G(K/\mathbb{Q})$ of f?

(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

[**4**] Repeat [**3**] for $f(x) = x^3 - 3x + 1$.

[**5**] Repeat [**3**] for $f(x) = x^4 - 3x^2 + 2$.

[**6**] Repeat [**3**] for $f(x) = x^4 - 5x^2 + 6$.

[**7**] Prove the primitive element theorem (14.4.1, p. 552): Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

[**8**] Prove the following theorem about Kummer extensions (14.7.4, p. 566): Let F be a subfield of $\mathbf{C}$ which contains the pth root of unity ζ for a prime p, and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root to F.

Practice Problems for Final Exam

Modern Algebra, Dave Bayer, May 3, 1999

Our final will be held on Wednesday, May 12, 1:10pm – 4:00pm, in our regular classroom. It will consist of 8 questions worth 40 points in all. Two questions will be review from previous exams, and the remaining six questions will test material since the last exam.

The following two problems constitute the review topics from previous exams.

[1] (compare with midterm 1, problem 5) Let $\mathbf{X} \subset \mathbb{R}^2$ be a finite set of points. Define $I \subset \mathbb{R}[x, y]$ to be the set of all polynomials $f(x, y)$ that vanish on every point of $\mathbf{X}$. That is,

$$I \quad = \quad \{\ f(x,y) \in \mathbb{R}[x,y] \ \mid\ f(a,b) = 0 \ \text{ for every point } \ (a,b) \in X\ \}.$$

Prove that I is an ideal.

[2] (midterm 2, problem 2) What is the minimal polynomial of $\alpha = \sqrt{-1} + \sqrt{2}$ over $\mathbf{Q}$? (Note that we now have another way to compute this; see Artin, p. 554, discussion after proof of Proposition 14.4.4.)

The following problems are taken from last year's review questions for the final.

[3] Let $f(x, y, z) = x^2y + x^2z + xy^2 + y^2z + xz^2 + yz^2$. Express $f(x)$ as a polynomial $g(\sigma_1, \sigma_2, \sigma_3)$ where σ_1, σ_2, σ_3 are the elementary symmetric functions

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + xz + yz, \quad \sigma_3 = xyz.$$

[4] Let $f(x) = x^2 + ax + b$ have roots α_1 and α_2, where

$$\alpha_1 + \alpha_2 = c, \qquad \alpha_1^2 + \alpha_2^2 = d.$$

Express a and b in terms of c and d.

Recall that the discriminant of $f(x) = x^2 + bx + c$ is $D = b^2 - 4c$, and that the discriminant of $f(x) = x^3 + px + q$ is $D = -4p^3 - 27q^2$.

[5] Let $f(x) = x^3 - 2$.
(a) What is the degree of the splitting field K of f over $\mathbf{Q}$?
(b) What is the Galois group $G = G(K/\mathbf{Q})$ of f?
(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

[6] Repeat for $f(x) = x^3 - 3x + 1$.

[7] Repeat for $f(x) = x^4 - 3x^2 + 2$.

[8] Repeat for $f(x) = x^4 - 5x^2 + 6$.

[9] Prove the primitive element theorem (14.4.1, p. 552): Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

[10] Prove the following theorem about Kummer extensions (14.7.4, p. 566): Let F be a subfield of $\mathbf{C}$ which contains the pth root of unity ζ for a prime p, and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root to F.

The following problems are taken from last year's final.

[11] Prove that $\alpha = e^{2\pi i/11} + 3$ is not constructible.

[12] What is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$?

[13] Let $f(x, y, z) = x^3 + y^3 + z^3$. Express $f(x)$ as a polynomial $g(\sigma_1, \sigma_2, \sigma_3)$ where σ_1, σ_2, σ_3 are the elementary symmetric functions

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + xz + yz, \quad \sigma_3 = xyz.$$

Recall that the discriminant of $f(x) = x^2 + bx + c$ is $D = b^2 - 4c$, and that the discriminant of $f(x) = x^3 + px + q$ is $D = -4p^3 - 27q^2$.

[14] Let $f(x) = x^3 - 12$.
(a) What is the degree of the splitting field K of f over $\mathbf{Q}$?
(b) What is the Galois group $G = G(K/\mathbf{Q})$ of f?
(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

[15] Prove the primitive element theorem (14.4.1, p. 552): Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

Final Examination

Dave Bayer, Modern Algebra, May 13, 1998

[1] Which of the following rings are integral domains? Explain your reasoning.
(a) $\mathbb{F}_2[x]/(x^4 + x^2 + 1)$
(b) $\mathbb{Q}[x]/(x^4 + 2x^2 + 2)$

[2] Consider the ideal $I = (2, 3x^2) \subset \mathbb{Z}[x]$, and let $R = \mathbb{Z}[x]/I$.
(a) Does $f(x) = 7x^4 + 5x^3 + 3x^2 + 2x$ belong to I?
(b) How many elements are there in R?
(c) List representatives for the elements of R, and describe the multiplication rule in R for these representatives.

[3] Let R be a principal ideal domain, and let

$$I_1 \quad \subset \quad I_2 \quad \subset \quad I_3 \quad \subset \quad \cdots \quad \subset \quad I_n \quad \subset \quad \cdots$$

be an infinite ascending chain of ideals in R. Show that this chain *stabilizes*, i.e.

$$I_N \quad = \quad I_{N+1} \quad = \quad I_{N+2} \quad = \quad \cdots$$

for some N.

[4] Working in the Gaussian integers $\mathbb{Z}[i]$, factor 2 into primes.

[5]
(a) Give a presentation of the finite field with 27 elements $\mathbb{F}_{27}$, of the form $\mathbb{F}_3[x]/(f(x))$.
(b) In terms of this presentation, guess a generator α of the multiplicative group $\mathbb{F}_{27}^*$. Compute the odds that such a guess is correct. Explain your reasoning.

[6] Prove that $\alpha = e^{2\pi i/11} + 3$ is not constructible.

[7] What is the minimal polynomial of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$?

[8] Let $f(x, y, z) = x^3 + y^3 + z^3$. Express $f(x)$ as a polynomial $g(\sigma_1, \sigma_2, \sigma_3)$ where σ_1, σ_2, σ_3 are the elementary symmetric functions

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + xz + yz, \quad \sigma_3 = xyz.$$

Recall that the discriminant of $f(x) = x^2 + bx + c$ is $D = b^2 - 4c$, and that the discriminant of $f(x) = x^3 + px + q$ is $D = -4p^3 - 27q^2$.

[9] Let $f(x) = x^3 - 12$.

(a) What is the degree of the splitting field K of f over $\mathbb{Q}$?

(b) What is the Galois group $G = G(K/\mathbb{Q})$ of f?

(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

[10] Prove the primitive element theorem (14.4.1, p. 552): Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

Final Exam

Modern Algebra, Dave Bayer, May 12, 1999

Name: ______________________________

ID: ____________________ **School:** ____________________

[**1**] (5 pts)	[**2**] (5 pts)	[**3**] (5 pts)	[**4**] (5 pts)	
[**5**] (5 pts)	[**6**] (5 pts)	[**7**] (5 pts)	[**8**] (5 pts)	**TOTAL**

Please work only one problem per page, and label all continuations in the spaces provided. Extra pages are available. Check your work, where possible.

[**1**] Let $\mathbf{X} = \{a_1, \ldots, a_n\} \subset \mathbb{C}$ be a finite set of points, where $\mathbb{C}$ is the complex numbers. Define $I \subset \mathbb{C}[x]$ to be the set of all polynomials $f(x)$ that vanish on every point of $\mathbf{X}$. That is,

$$I \quad = \quad \{\ f(x) \in \mathbb{C}[x] \ \mid \ f(a_i) = 0 \ \text{ for every point } \ a_i \in \mathbf{X}\ \}.$$

(a) Prove that I is an ideal.

(b) Give a set of generators for I.

 Continued on page: ______

Problem: ______

Continued on page: ______

[2] What is the minimal polynomial of $\alpha = \sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$?

 Continued on page: ______

Problem: ______

Continued on page: ______

[3] Let $f(x, y, z) = x^3yz + xy^3z + xyz^3$. Express $f(x)$ as a polynomial $g(\sigma_1, \sigma_2, \sigma_3)$ where σ_1, σ_2, σ_3 are the elementary symmetric functions

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + xz + yz, \quad \sigma_3 = xyz.$$

Continued on page: ______

Continued on page: ______

[4] Prove the primitive element theorem: Let K be a finite extension of a field F of characteristic zero. There is an element $\gamma \in K$ such that $K = F(\gamma)$.

 Continued on page: ______

Problem: ______

Continued on page: ______

[5] Prove the following theorem about Kummer extensions: Let F be a subfield of $\mathbb{C}$ which contains the pth root of unity ζ for a prime p, and let K/F be a Galois extension of degree p. Then K is obtained by adjoining a pth root to F.

 Continued on page: ______

Problem: ______

Continued on page: ______

Recall that the discriminant of $f(x) = x^3 + px + q$ is $D = -4p^3 - 27q^2$.

[**6**] Let $f(x) = x^3 + 2$.

(a) What is the degree of the splitting field K of f over $\mathbb{Q}$?

(b) What is the Galois group $G = G(K/\mathbb{Q})$ of f?

(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

 Continued on page: ______

Problem: ______

Continued on page: ______

[7] Let $f(x) = x^3 + x - 2$.

(a) What is the degree of the splitting field K of f over $\mathbb{Q}$?

(b) What is the Galois group $G = G(K/\mathbb{Q})$ of f?

(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

 Continued on page: ______

Problem: ______

Continued on page: ______

[**8**] Let $f(x) = x^5 - 1$.

(a) What is the degree of the splitting field K of f over $\mathbb{Q}$?

(b) What is the Galois group $G = G(K/\mathbb{Q})$ of f?

(c) List the subfields L of K, and the corresponding subgroups $H = G(K/L)$ of G.

 Continued on page: ______

Problem: ______

Continued on page: ______