Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
January 2016

Do 6 problems with at least 2 in each section.

Group theory problems:

(1) Let G be a group. Consider the commutator subgroup $[G, G]$ of G, the subgroup generated by all commutators, $aba^{-1}b^{-1}$ where $a, b \in G$. It is known that $[G, G]$ is a normal subgroup of G. Prove that
- $G/[G, G]$ is Abelian, and
- if $K \trianglelefteq G$ such that G/K is Abelian, then $[G, G] \trianglelefteq K$.

(2) Let $(G, \cdot)$ be a group and $Z = Z(G)$ its center. Suppose that the group G/Z is cyclic. Show that G is Abelian.

(3) Prove that any finite group is isomorphic to a subgroup of A_n for some n, where A_n is the alternating group on n elements. (Consider Cayley's Theorem.)

Ring theory problems:

(1) Prove that every prime ideal is maximal in a PID.

(2) Let R be a commutative ring. Prove that the following are equivalent:
(i) R is a field;
(ii) $R \neq \{0\}$ and the only ideals of R are $\{0\}$ and R.

(3) Let R be a commutative ring with 1. For any two ideals I and J of R, let IJ be the ideal generated by all products xy where $x \in I$ and $y \in J$. Suppose $I + J = R$, prove that $IJ = I \cap J$.

Field theory problems:

(1) (a) Find the degree $[F : \mathbb{Q}]$ of the extension $F = \mathbb{Q}(i, \sqrt{3})$ over $\mathbb{Q}$. Find a basis of the vector space F over $\mathbb{Q}$.
(b) Find a primitive element of the extension F of $\mathbb{Q}$.

(2) (a) Identify $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, the group of all automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ which fix $\mathbb{Q}$.
(b) Determine if the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is Galois.

(3) Prove that for any prime p, the field $\mathbb{F}_p$ with p elements contains an element a such that $[\mathbb{F}_p(\sqrt[3]{a}) : \mathbb{F}_p] = 3$ if and only if 3 divides $p - 1$ (Hint: you may use the fact that for any finite field F, the multiplicative group F^* is cyclic.)

Ph.D. Qualifying Examination in Algebra

Department of Mathematics

University of Louisville

August 2015

Do 6 problems with at least 2 in each section.

Group theory problems:

(1) Let G be an arbitrary group. For any two subgroups H and K of G, define $HK = \{hk : h \in H, k \in K\}$. Assume $H \trianglelefteq G$ and $K \leq G$, where $\leq$ denotes a subgroup and $\trianglelefteq$ denotes a normal subgroup.

   (a) Prove that $HK \leq G$.

   (b) Prove that $H \trianglelefteq HK$ and $(H \cap K) \trianglelefteq K$.

   (c) Prove that $\frac{HK}{H} \cong \frac{K}{H \cap K}$.

(2) (a) Consider the cyclic group $(\mathbb{Z}_{10}, +)$, where $\mathbb{Z}_{10} = \{\overline{0}, \overline{1}, \ldots, \overline{9}\}$ and the addition is modulo 10. If f is an automorphism of this group, what are all possible values of $f(\overline{1})$? Explain. Find all automorphisms of this group.

   (b) A subgroup N of a group G is called a *characteristic subgroup* if $\phi(N) = N$ for all automorphisms ϕ of G. Prove that every subgroup of the group $(\mathbb{Z}_{10}, +)$ is characteristic.

(3) Prove that a group of order 300 cannot be simple.

Ring theory problems:

(1) A ring R (not necessarily commutative) with identity $1_R \neq 0$ in which every nonzero element is a unit is called a *division ring*. Prove that a ring R with identity 1_R is a division ring if and only if R has no proper left ideal.

(2) Let A and B be ideals of a ring R with $B \subseteq A$.

   (a) Show that $A/B = \{a + B \mid a \in A\}$ is an ideal of the ring R/B.

   (b) Show that the map $f : R/B \to R/A$, given by $f(x + B) = x + A$ for every $x \in R$, is well-defined, onto and a homomorphism.

   (c) Show that $(R/B)/(A/B)$ is isomorphic to R/A.

(3) Let R be a commutative ring and I an ideal of R. Let (I, X) be the ideal of $R[X]$ generated by $I \cup \{X\}$.

(a) Prove that (I, X) consists precisely of all the polynomials in $R[X]$ whose constant term belongs to I.

(b) For any maximal ideal M of R, prove that (M, X) is a maximal ideal of $R[X]$.

Field theory problems:

(1) Let $F = \mathbb{Q}(i, \sqrt{3})$, where $i = \sqrt{-1}$. Find the degree of the extension $[F : \mathbb{Q}]$ and a (vector space) basis of F over $\mathbb{Q}$. Justify your answer.

(2) Let F be a field and let $f(x) \in F[x]$.

(a) What is the definition of the *splitting field* of the polynomial $f(x)$ over the field F?

(b) Let $a \in F$. Show that $f(x)$ and $f(x + a)$ have the same splitting field over F.

(3) Determine the splitting field and its degree over $\mathbb{Q}$ for the polynomial $X^6 - 4$. Justify your answer.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
January 2015

This exam consists of three parts. For each part select two problems and work on them. If you work more problems, clearly indicate which two should be graded. Please write on one side of each sheet of paper and put your name in the upper right hand corner.

Group theory problems:

(1) If N is a normal subgroup of G and H is any subgroup of G, prove that $NH := \{nh \mid n \in N, h \in H\}$ is a subgroup of G.

(2) Let G be an arbitrary group with a center $Z(G)$. Prove that the inner automorphism group $Inn(G)$ is isomorphic to $G/Z(G)$. (Recall: by definition, $Inn(G)$ is the group of all automorphisms ϕ_h of the form $\phi_h(g) = h^{-1}gh$, $\forall g \in G$).

(3) Let G be a finite group and suppose that $H \trianglelefteq G$. Prove that for any Sylow p-subgroup P of G, $P \cap H$ is a Sylow p-subgroup of H.

(4) Show that a group of order 56 is not simple.

Ring theory problems:

(1) Let $f : R \to S$ be a homomorphism of rings, I an ideal in R, and J an ideal in S.

(a) Prove that $f^{-1}(J) = \{x \in R : f(x) \in J\}$ is an ideal in R and that this ideal contains $Ker\ f$.

(b) Prove that if f is surjective (i.e., onto), then $f(I) = \{f(y) : y \in I\}$ is an ideal in S. Give an example to show that $f(I)$ need not be an ideal in S when f is not surjective (i.e., onto).

(2) A ring R is called *Boolean* if every element is idempotent, that is $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

(3) Let R be a commutative ring with unity and let $P \neq R$ be an ideal of R. Prove that the following are equivalent:

i. P is prime.
ii. For any ideals I, J in R, if $IJ \subseteq P$ then $I \subseteq P$ or $J \subseteq P$.

(4) Show that every prime element in an integral domain is irreducible.

Field theory problems:

(1) Let E be a finite extension of the field F. Prove that E is algebraic over F.

(2) Find the degree of the extension $[F : \mathbb{Q}]$, where $F = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$. Is this a simple extension? Why or why not?

(3) Prove or provide a counterexample: Galois extensions of Galois extensions are Galois extensions. That is, if K/F is Galois and L/K is Galois, then L/F is Galois.

(4) Determine the Galois group of $f(x) = x^4 - 5x^2 + 6$ over $\mathbb{Q}$. (Recall that the Galois group of a separable polynomial $f(x) \in F[x]$ is defined to be the Galois group of the splitting field of $f(x)$ over F.)

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
August 2014

Do 6 problems with at least 2 in each section.

Group theory problems:

(1) Let G be a group of order 56. Prove that G is not simple.

(2) Suppose that G is a finite group with even order. Prove that the number of conjugacy classes in G with odd order is even.

(3) Let $H \leq G$. Prove that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$. Recall the normalizer $N_G(H) = \{g \in G | gHg^{-1} = H\}$ and the centralizer $C_G(H) = \{g \in G | gh = hg, \forall h \in H\}$.

Ring theory problems:

(1) An integral domain D is said to be **Artinian** if for any descending chain of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$$

of D, there is an integer n such that $I_i = I_n$ for all $i \geq n$. Prove that an integral domain D is Artinian if and only if it is a field.

(2) Let R be a commutative ring with 1 . Let $e \in R$ be an idempotent element (that is, $e^2 = e$). Show that $R \cong eR \times (1 - e)R$.

(3) A *principal ideal ring* is a ring in which every ideal has a single generator.
   (a) Prove that an element of a principal ideal domain is prime if and only if it is irreducible.
   (b) Provide an example of a principal ideal ring containing an element which is prime but not irreducible.

Field theory problems:

(1) Let E be a finite extension of the field F. Prove that E is algebraic over F.

(2) Let $a = \sqrt{1 + \sqrt{2}}$ and put $E = \mathbb{Q}(a)$.
   (a) Find the minimal polynomial of a over $\mathbb{Q}$.
   (b) Find $[E : \mathbb{Q}]$.
   (c) Identify the group $Gal(E/\mathbb{Q})$, the set of all automorphisms of E which fix $\mathbb{Q}$.

(3) Let K be an extension field of F and let $\alpha \in K$. Prove that if α is transcendental over F, then $F(\alpha) \neq F(\alpha^2)$. Provide an example showing the reverse implication false.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics

University of Louisville

January 2014

Do 7 problems with at least 2 in each section.

Group theory problems:

(1) There are five nonisomorphic groups of order 12 (you may take this as given). List them all, and show that the groups you listed are mutually nonisomorphic.

(2) Let G be a group, and let $[G, G]$ be the subgroup of G *generated by* $\{aba^{-1}b^{-1} : a, b \in G\}$. (So $[G, G]$ is the *commutator subgroup* of G.)

   (a) Prove that $[G, G]$ is a normal subgroup of G.

   (b) Let N be a normal subgroup of G. Prove that G/N is Abelian if and only if $[G, G] \subseteq N$.

(3) Suppose G is a group acting on a set X. For $a \in X$, let $O(a) = \{g(a) : g \in G\}$, the *orbit of* a under the action of G on X. Also, for $a \in X$, let $G_a = \{g \in G : g(a) = a\}$, the *stabilizer of* a in G. Let $\mathcal{O} = \{O(a) : a \in X\}$ be the set of orbits, and let $G/G_a = \{hG_a : h \in G\}$ be the set of all left cosets of G_a in G. (Note that G/G_a is not a group since G_a is not in general a normal subgroup of G.)

   (a) Suppose that $a \in X$. Prove that G_a is a subgroup of G.

   (b) Explicitly define a bijection ϕ from G/G_a to $O(a)$. You need to justify that ϕ is well defined, and is both one-to-one and onto.

   (c) Let G act on itself by conjugation. Suppose p is a prime number and G is a finite p-group, then G has a non-trivial center. Suggestion: By (b), it follows that the size of any orbit is a power of p.

(4) Show that A_8 has no subgroup of index 7. (hint: use the fact that A_8 is a simple group)

Ring theory problems:

(1) Let R be a commutative ring with identity. For any two ideals I and J of R, let IJ be the ideal generated by all products xy where $x \in I$ and $y \in J$.

   (a) Suppose that P is a prime ideal of R and that $IJ \subseteq P$. Show that either $I \subseteq P$ or $J \subseteq P$.

   (b) Suppose $I + J = R$, show that $IJ = I \cap J$.

(2) Let R be a ring (not necessarily commutative). Recall that a *right ideal* I of R is a non-empty subset of R that is closed under $-$, and for all $a \in R$, $Ra \subseteq I$. (This problem has two parts.)

   (a) Suppose that R is a ring with identity, and that the only right ideals of R are $\{0\}$ and R. Prove that R is a division ring. (That is, each

non-0 element $a \in R$ has a multiplicative inverse a^{-1}.)

(b) Suppose that R does **not** have an identity 1, and that the only right ideals of R are $\{0\}$ and R. Prove that R has trivial multiplication; that is, for all $a, b \in R$, we have $ab = 0$.

(3) Let D be the integral domain $\mathbb{Z}[\sqrt{-5}]$.
(a) Show that 2 is an irreducible element of D.

(b) Show that 2 is not a prime element of D.

(c) Show that D is not a UFD (unique factorization domain).

Field theory problems

(1) Let $L \subseteq \mathbb{C}$ be a finite Galois extension of $\mathbb{Q}$ with Galois group G. Suppose that G has odd order.
(a) Show that $L \subseteq \mathbb{R}$.

(b) Is the converse true? In other words, if $L \subseteq \mathbb{R}$ is a finite Galois extension of $\mathbb{Q}$ with the Galois group G, then must the order of G be odd?

(c) Give an explicit example of an extension L of $\mathbb{Q}$ such that L has degree 3 over $\mathbb{Q}$, $L \subseteq \mathbb{C}$, and $L \not\subseteq \mathbb{R}$.

(2) Let $K \leq N$ be a field extension, with N algebraic over K. Suppose that L is a subring of N, and that K is contained in L.
(a) Prove that L is a field.

(b) Find a field extension $A \leq C$ such that C contains a subring B, B contains A, but B is not a field. Provide an element $b \in B$ whose inverse is not contained in B.

(3) Let $q(x) = x^4 + 1$.
(a) Show that $q(x)$ is irreducible over $\mathbb{Q}$. (Note that is not enough to state that $q(x)$ has no real root.)

(b) Determine the four roots of $q(x) = x^4 + 1$.

(c) Let S be the splitting field of $q(x) = x^4 + 1$ over $\mathbb{Q}$. Determine $[S : \mathbb{Q}]$. Justify your answer.

(d) Determine the Galois group of $q(x)$ over $\mathbb{Q}$. Justify your answer.

(4) Let $K \leq F$ be a finite field extension and assume both fields are of prime characteristic p.

(a) Prove that $[K^p : F^p] = [K : F]$. Here $F^p := \{a^p : a \in F\}$ and K^p is defined similarly.

(b) Use the above to show that $K = K^p$ if and only if $F = F^p$. (that is, K is a perfect field if and only if F is perfect)

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
August 2012

1 Groups

Do any two problems from this section.

1. For any group G, we denote by G^2 the subgroup of G generated by squares of elements in G. In other words,
$$G^2 = \langle \{x^2 : x \in G\} \rangle.$$
First, prove that G^2 is a normal subgroup of G. Second, prove that the factor group G/G^2 is abelian.

2. (a) If N is a normal subgroup of G and H is any subgroup of G, prove that $NH := \{nh \,|\, n \in N, h \in H\}$ is a subgroup of G.
(b) Moreover, if H is also a normal subgroup of G, prove that NH is a normal subgroup of G.

3. If G is a group, Z its center, and if G/Z is cyclic, prove that G must be abelian.

4. Show that groups of order 105 are not simple.

2 Rings

Do any two problems from this section.

1. Let $F[x]$ be a ring polynomials where the coefficients belong to the field F. Prove that every ideal in $F[x]$ is principal. Is this fact still true if we replace F with any commutative ring R? Justify your answer.

2. Consider the subring $R = \{a + bi\sqrt{3} \,|\, a, b \in \mathbb{Z}\}$ of $\mathbb{C}$.
(a) Show that the map $\varphi : R \to \mathbb{Z}$, given by
$$\varphi(a + bi\sqrt{3}) = a^2 + 3b^2,$$
satisfies the property
$$\varphi(uv) = \varphi(u)\varphi(v)$$
for all $u, v \in R$. Show also that $\varphi(u) > 3$ for every $u \in R$, unless $u \in \{0, 1, -1\}$.
(b) Use (a) to show that the only units of R are 1 and -1.
(c) Use (a) to show that the elements $2, 1 + i\sqrt{3}, 1 - i\sqrt{3}$ of R are irreducible. Deduce that R is not a unique factorization domain.

3. Let
$$D = \{\frac{r}{s} \in \mathbb{Q} \mid r, s \in \mathbb{Z}, s \text{ odd}, r, s \text{ relatively prime}\}.$$

   (a) Show that D is a subring of $\mathbb{Q}$.

   (b) Describe the units of D.

   (c) Show that D is a principal ideal domain.

4. Let R be a commutative ring with 1. Let $I_1, I_2, \cdots, I_n$ be ideals of R such that $I_i + I_j = R$ for any $i \neq j$. Show that there exists an isomorphism
$$R/(\bigcap_{i=1}^{n} I_i) \cong (R/I_1) \times \cdots \times (R/I_n).$$

3 Fields

Do any two problems from this section.

1. Find the minimal polynomial of $\alpha = \sqrt{3+\sqrt{7}}$ over the field $\mathbb{Q}$ of rational numbers, and *prove* it is the minimal polynomial.

2. (a) Show that the polynomial $X^2 + X + 1$ is irreducible over $\mathbb{Z}_2 = \{0, 1\}$.

   (b) Explain why the ideal $\langle X^2 + X + 1\rangle$ is a maximal ideal of $\mathbb{Z}_2[X]$ and why $K = \mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$ is a field.

   (c) List all the elements of K.

   (d) Are there two distinct elements α, β of K such that $\alpha^2 = \beta$? Explain.

3. Let $G = \text{Gal}(\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}), \mathbb{Q})$.

   (a) How many elements are there in G? Describe all of them.

   (b) Give a proper nontrivial subgroup H of G. Describe the subfield K of $\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3})$ consisting of the elements fixed by H. What is $[\mathbb{Q}(\sqrt[3]{5}, i\sqrt{3}) : K]$?

4. Assume both E/F and K/E are separable field extensions. Prove that K/F is separable.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
August 2011

This exam consists of three parts. For each part select two problems and work on them. If you work more problems, clearly indicate which should be graded. Please write on one side of each sheet of paper and put your name in the upper right hand corner.

1 Groups

1. Let $\mathbb{Z}$ denote the set of integers and let H denote the set of all 3×3 matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \quad x, y, z \in \mathbb{Z}$$

   Prove that H is a noncommutative group under matrix multiplication.

2. Let H and K be normal subgroups of a group G. Assume that $HK = G$ and $H \cap G = \{1\}$.
   (a) Prove that $hk = kh$ for any $h \in H$ and $k \in K$.
   (b) Prove that G is isomorphic to $H \times K$.

3. Determine up to isomorphism all Abelian groups of order 96.

4. Let S_n denote the group of permutations of the set $\{1, 2, \ldots n\}$. Find all the subgroups of S_3 and determine which of them are normal in S_3.

2 Rings

1. Let $f : R \to S$ be a homomorphism of rings, I an ideal in R, and J an ideal in S.

   (a) Prove that $f^{-1}(J) = \{x \in R : f(x) \in J\}$ is an ideal in R and that this ideal contains $Ker\ f$.

   (b) Prove that if f is onto, then $f(I) = \{f(y) : y \in I\}$ is an ideal in S. Give an example to show that $f(I)$ need not be an ideal in S when f is not onto.

2. Show that every prime element in an integral domain is irreducible.

3. A commutative ring with 1 is said to be *Artinian* if for every descending chain of ideals

   $$I_1 \supseteq I_2 \supseteq \cdots,$$

   there is an integer n such that $I_i = I_n$ for all $i \geq n$.

   Let R be an Artinian ring.

   (a) For every ideal I in R show that R/I is Artinian.

   (b) Show that every prime ideal in R is also a maximal ideal.

4. Consider the set $\Gamma = \{x + yi \,|\, x, y \in \mathbb{Z}\}$ of complex numbers, called *Gaussian integers*.

   (a) Show that Γ is an integral domain.

   (b) Find all the units of Γ.

   (c) It is known that Γ is, in fact, a Euclidean domain, and hence a unique factorization domain. Does

   $$13 = (2 + 3i)(2 - 3i) = (3 + 2i)(3 - 2i)$$

   contradict unique factorization in Γ?

   (d) Express 5 as a product of irreducible elements of Γ.

3 Fields

1. Prove that a finite integral domain is a field.

2. Let E denote the extension field $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

   (a) Find $[E : \mathbb{Q}]$, the degree of the extension.

   (b) Prove that $E = \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

   (c) Let S be the smallest field containing E which is normal over $\mathbb{Q}$. Find $[S : E]$.

3. (a) Show that the polynomial $X^4 - 2$ is irreducible over $\mathbb{Q}$.

   (b) Find a factorization of $X^4 - 2$ into linear factors over $\mathbb{C}$. Find the splitting field F of $X^4 - 2$.

   (c) Find the degree of F over $\mathbb{Q}$. Justify.

4. (a) Explain why $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a normal extension of $\mathbb{Q}$.

   (b) How many elements are there in the Galois group $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$? Define all of them.

   (c) Which well-known group is $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$ isomorphic to?

   (d) Which subgroup of $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$ has $\mathbb{Q}(\sqrt{6})$ as the corresponding fixed subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$?

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Summer 2009

1 Groups

Do any two problems from this section.

1. Let K and H be groups. Consider the group $K \times H$, the direct product of K and H. Determine whether the statements below are true or false. If true, provide a proof; otherwise provide a specific counterexample.

   (a) If K and H are both cyclic, then $K \times H$ is cyclic.

   (b) If K and H are both solvable, then $K \times H$ is solvable.

   (c) If K and H are both simple, then $K \times H$ is simple.

2. Let G be a group.

   (a) Prove that if H is a subgroup of G such that $|G : H| = 2$, then H is normal in G.

   (b) Prove that if G is infinite, then G has infinitely many subgroups.

3. Let G be a group under the operation $*$. Let u be an element of G. Define a new binary operation $\circ$ on G as follows: $a \circ b = a * u * b$, for all $a, b \in G$.

   (a) Prove that $\circ$ is associative.

   (b) Show that G contains an identity element under $\circ$; identify this element explicitly.

   (c) Show that every element of G contains an inverse under $\circ$.

   (d) True or False: "The groups $(G, *)$ and $(G, \circ)$ are isomorphic." Justify your answer by either exhibiting an isomorphism or giving a specific counterexample.

4. Show that, if $f : G \to H$ is a surjective group homomorphism and K is a normal subgroup of G, then $f(K)$ is a normal subgroup of H and $H/f(K) \cong G/K$.

2 Rings

Do any two problems from this section.

1. Let F be a field. Answer the following; justify your answers.

   (a) Describe all maximal ideals of $K[x]$.

   (b) Describe all prime ideals of $K[x]$.

   (c) Give an example of some field K and some polynomial $f \in K[x]$ such that $K[x]/(f(x))$ is not an integral domain.

   (d) Give an example of some field K and some polynomial $f \in K[x]$ such that $K[x]/(f(x))$ is a field.

2. Answer all four parts of this question.

   (a) State Eisenstein's criterion for an integral domain R.

   (b) Prove that $2x^5 - 6x^3 + 9x^2 - 15$ is irreducible in $\mathbb{Q}[x]$.

   (c) Use the substitution $y = x+1$ to prove that, if p is a prime integer, then
   $$x^{p-1} + x^{p-2} + \cdots + x + 1$$
   is irreducible in $\mathbb{Q}[x]$.

   (d) Prove or disprove that $g(x, y) = x^3+y^3+1$ is irreducible in $\mathbb{C}[x, y]$.

3. Recall that $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ and that $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. You may assume that both are integral domains.

   (a) What are the units of $\mathbb{Z}[i]$?

   (b) What are the units of $\mathbb{Z}[\sqrt{-5}]$?

   (c) Is 2 irreducible in $\mathbb{Z}[i]$? Is 2 irreducible in $\mathbb{Z}[\sqrt{-5}]$?

   (d) The ring $\mathbb{Z}[i]$ is a unique factorization domain, a fact you can assume is true. Notice that $5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i)$. Does the existence of these two factorizations of 5 into a product of primes in $\mathbb{Z}[i]$ contradict that $\mathbb{Z}[i]$ is a Unique Factorization Domain? Why?

3 Fields

Do any two problems from this section.

1. Let a and b be distinct prime numbers.
   (a) Prove that $\mathbb{Q}(\sqrt{a}+\sqrt{b}) = \mathbb{Q}(\sqrt{a},\sqrt{b})$.
   (b) Using (a), prove that $\left[\mathbb{Q}(\sqrt{a}+\sqrt{b}) : \mathbb{Q}\right] = 4$.
2. Answer the following with your justification.
   (a) What is the splitting field K of $x^8 - 1$ over $\mathbb{Q}$?
   (b) Find the minimal polynomial of K over $\mathbb{Q}$?
   (c) Find $\mathrm{Gal}(K/\mathbb{Q})$?
3. Let K be an extension of the field F. Show that the elements in K that are algebraic over F form a subfield of K.
4. Answer the following with your justification.
   (a) Exhibit an irreducible polynomial of degree 3 in $\mathbb{Z}_3[x]$.
   (b) Use (a) to prove that there exists a finite field with 27 elements.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2008

1 Groups

Do any two problems from this section.

1. Show that if G is a cyclic group then every subgroup of G is cyclic.

2. Let G be a group and $Z(G)$ be its center. Prove that if $G/Z(G)$ is cyclic then G is Abelian.

3. Let H and N be subgroups of a group G with N normal. Prove that $NH = HN$ and that this set is a subgroup of G. (Here $NH = \{nh | n \in N, h \in H\}$, $HN = \{hn | h \in H, n \in N\}$.)

2 Rings

Do any two problems from this section.

1. Let $\mathbb{Z}$ be the ring of integers. Prove that the polynomial ring $\mathbb{Z}[x]$ is not a principal ideal domain. Is it a unique factorization domain?

2. Prove that every nonzero prime ideal in a principal ideal domain is a maximal ideal.

3. Show that a proper ideal M in a commutative ring R is maximal if and only if for every $r \in R \setminus M$ there exists $x \in R$ such that $1 - rx \in M$.

3 Fields

Do any two problems from this section.

1. If F is a finite dimensional extension field of K, then prove that F is finitely generated and algebraic over K.

2. Let $f(x) = x^4 - 2$ over $\mathbb{Q}$.
   (a) Find the splitting field K of $f(x)$ over $\mathbb{Q}$.
   (b) Find the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$.
   (c) Draw the diagram of the subgroups of G and the diagram of corresponding fixed fields.

3. Show that the polynomial $g(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible in $\mathbb{Z}_2[x]$. Using this polynomial construct a field of four elements. Construct the addition and the multiplication table for this field.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Summer 2008

1 Groups

Do any two problems from this section.

1. Show that a group of order $1000 = 2^4 \cdot 5^4$ cannot be simple.

2. Let K be a normal subgroup of a group G and suppose that K has exactly two elements. Show that K is contained in the center $Z(G)$ of G.

3. Prove that if H is a normal subgroup of a group G of prime index p, then for all $K \leq G$ either
   (i) $K \leq H$ or
   (ii) $G = HK$ and $|K : K \cap H| = p$.

2 Rings

Do any two problems from this section.

1. Let $R = C[0,1]$ be the set of all continuous real-valued functions on $[0,1]$. Define addition and multiplication on R as follows. For $f, g \in R$ and $x \in [0,1]$,

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

a) Show that R with these operations is a commutative ring with identity.

b) Find the units of R.

c) If $f \in R$ and $f^2 = f$, then show that $f = 0_R$ or $f = 1_R$.

2. In the ring $\mathbb{Z}$ of integers the following conditions on a nonzero ideal I are equivalent: (i) I is prime; (ii) I is maximal; (iii) $I = (p)$ with p prime.

3. Consider the ring $\mathbb{Z}[i]$ of Gaussian integers.

(a) Show that any prime $p \in \mathbb{Z}$ with $p \equiv 3 \pmod 4$ is irreducible over $\mathbb{Z}[i]$.

(b) Prove that $f(x) = x^3 + 12x^2 + 18x + 6$ is irreducible over $\mathbb{Z}$ and over $\mathbb{Z}[i]$.

3 Fields

Do any two problems from this section.

1. Let F be a field. Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

2. Let $f(x) = x^4 - 5x^2 + 6$ over $\mathbb{Q}$.
(a) Find the splitting field K of $f(x)$ over $\mathbb{Q}$.
(b) Find the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$.
(c) Draw the diagram of the subgroups of G and the diagram of corresponding fixed fields.

3. Let F be a finite field with multiplicative identity 1_F. Prove that when you multiply all the nonzero elements of F, then the answer is -1_F. (Here -1_F is the additive inverse of 1_F.)

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2007

1 Groups

Do any two problems from this section.

1. Classify up to isomorphism all groups of order 175.

2. Let H and N be subgroups of a group G with N normal. Prove that $NH = HN$ and that this set is a subgroup of G.

3. Do two parts to receive full credit.

   (a) Let G be the multiplicative group of all nonsingular 2×2 matrices with rational numbers. Show that $g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ has order 4 and $h = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ has order 3, but that gh has infinite order.

   (b) Show that the additive group $H = (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$ contains nonzero elements a, b of infinite order such that $a + b$ is nonzero and has finite order.

4. Prove that every finitely generated subgroup of the additive group of rational numbers is cyclic.

2 Rings

Do two problems from this section. **One problem should include either Problem 1 or 2 (but not both)**.

1. The following is a well known fact: if K is a commutative ring with identity and I is an ideal of K, then K/I is a field if and only if I is a maximal ideal of K. Answer all the parts to receive full credit.

   (a) Find all the maximal ideals of $\mathbb{Z}$. (You may use the fact that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.)

   (b) Determine whether the ideal $(3, x)$ is a maximal ideal in $\mathbb{Z}[x]$.

   (c) Determine whether the ideal (x) is a maximal ideal in $\mathbb{Z}[x]$.

2. Do all the parts to receive full credit.

   (a) Define *prime ideal* and *maximal ideal* in a commutative ring R with identity.

   (b) Let R and S be commutative rings with identities 1_R and 1_S, respectively, and let $f : R \to S$ be a ring homomorphism such that $f(1_R) = 1_S$. If P is a prime ideal of S show that $f^{-1}(P)$ is a prime ideal of R.

   (c) Let f be as in part (b). If M is a maximal ideal of S, is $f^{-1}(M)$ a maximal ideal of R? Prove that it is or give a counter example.

3. Let

$$A = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a + c = b + d, \quad a, b, c, d \in \mathbb{Z} \right\}.$$

   It is easy to see that A is a subring of $M_2(\mathbb{Z})$ (the ring of 2×2 matrices with elements from $\mathbb{Z}$). Do the two parts to receive full credit.

   (a) Let R be the ring of 2×2 lower triangular matrices $\begin{bmatrix} m & 0 \\ n & p \end{bmatrix}$ with elements from $\mathbb{Z}$. Consider the map $f : R \to A$ defined by

$$f\left(\begin{bmatrix} m & 0 \\ n & p \end{bmatrix} \right) = \begin{bmatrix} m-n & m-n-p \\ n & n+p \end{bmatrix}.$$

   Is f a homomorphism of rings? Justify the answer.

   (b) Are the rings R and A isomorphic? Explain.

4. Show that a proper ideal M in a commutative ring R is maximal if and only if for every $r \in R \setminus M$ there exists $x \in R$ such that $1 - rx \in M$.

3 Fields

Do any two problems from this section.

1. Prove that $\mathbb{Q}(\sqrt{3}+\sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Describe the lattice of subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$ and the lattice of subfields of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

2. Do all the parts to receive full credit.

   (i) Show that $g = X^3 - 3X - 1$ is an irreducible polynomial over $\mathbb{Q}$.

   (ii) It is known that there is a simple extension field $\mathbb{Q}(u)$ of $\mathbb{Q}$ such that u is a root of g and $[\mathbb{Q}(u) : \mathbb{Q}] = 3$. How is $\mathbb{Q}(u)$ defined? List the elements of a basis of $\mathbb{Q}(u)$ over $\mathbb{Q}$.

   (iii) Show that there exists a splitting extension K of g with $[K : \mathbb{Q}] \leq 6$.

3. Prove that one of $2, 3$ or 6 is a square in the finite field $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

   has a root modulo p for every prime p but has no root in $\mathbb{Z}$.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2006

1 Groups

Do any two problems from this section.

1. Let G be a group of order $5^2 7^2$.

   (a) Using the Sylow Theorems, show that G is Abelian.

   (b) Determine all isomorphism types of Abelian groups of order $5^2 7^2$.

2. Let G be a finite group with exactly three conjucacy classes. Show that exactly one of the following possibilities holds:

   (a) $|G| = 3$.

   (b) $|G| = 6$ and G is non-Abelian.

3. Prove that an infinite group is cyclic if and only if it is isomorphic to each of its proper non-trivial subgroups.

4. Let G be a finite group.

   (a) State the Class Equation for G in a form that involves the center $Z(G)$ of G and the index of centralizers of elements of G.

   (b) Determine the conjugacy class of S_4 and their orders. Then verify the Class Equation, given in part (a), is valid for S_4.

   (c) Let p be a prime number and let G be a non-trivial p-group. Use the Class Equation to show that G has a non-trivial center.

5. Prove that if a group G is nilpotent, then it is solvable.

2 Rings

Do any two problems from this section.

1. Do both.

   (a) Prove that if F is a field, then the polynomial ring $F[x]$ is a Euclidean domain. That is, $F[x]$ is an integral domain and there exists a function $\phi : F[x] - \{0\} \to \mathbb{N}$ such that if $f, g \in F[x]$ and $g \neq 0$, then there exist $q, r \in F[x]$ such that $f = qg + r$ with $r = 0$ or $\phi(r) < \phi(g)$.

   (b) Prove or disprove that if R is an integral domain and A is a proper ideal of R, then R/A is an integral domain.

2. Do both.

   (a) Show that $\mathbb{Z}[i]/(3+i)$ is isomorphic to $\mathbb{Z}/10\mathbb{Z}$.

   (b) Is $(3+i)$ a maximal ideal of $\mathbb{Z}[i]$? Give a reason for your answer.

3. Let R, S be rings and let $f : R \to S$ be a surjective ring homomorphism (that is, $f(R) = S$). Let $Ker(f)$ be the kernel of f.

   Define $f^* : R/Ker(f) \to S$ as follows: $f^*(a + Ker(f)) = f(a)$.

   (a) Show that f^* is well-defined.

   (b) Show that $f^* : R/Ker(f) \to S$ is a bijection.

   (c) Show that $f^* : R/Ker(f) \to S$ is a ring homomorphism.

3 Fields

Do two problems from this section with one of the problems being problem 3

1. Do both.

   (a) Prove that $F = \{\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : \ a, b \in \mathbb{Q}\}$ is a field under matrix addition and multiplication.

   (b) Prove that F is isomorphic to the field $\mathbb{Q}(\sqrt{2})$.

2. Given $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

   (a) Show that $f(x)$ is irreducible over $\mathbb{Z}_2$.

   (b) Let $F = \mathbb{Z}_2[x]/\langle f(x)\rangle$ and α be a zero of $f(x)$ in F. Show that for each nonzero element β of F, there exists a polynomial $q(x) \in Z_2[x]$ of degree at most 2 such that $\beta = q(\alpha)$.

3. Consider $p(x) = x^3 + 5 \in Q[x]$. Let S be the splitting field of $p(x) \in Q[x]$ and assume S is contained in $\mathcal{C}$, the field of complex numbers. You will be graded on the correctness and thoroughness of your explanations: provide relevant theorems, facts etc. to support each of your assertions.

   (a) Determine $[S : Q]$, showing all details.

   (b) Determine $Gal(S/Q)$, up to isomorphism. Provide thorough explanation, citing relevant theorems, facts, etc. to support your conclusions.

   (c) Explain why S contains exactly one subfield J, with $Q \leq J \leq S$, such that $[J : Q] = 2$.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2005

1 Groups

Do any two problems from this section.

1. Prove that a group that has only a finite number of subgroups must be finite.

2. Prove that $G = \{\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \text{ real and } a > 0\}$ is a group under matrix multiplication. Show that G contains a subgroup H such that H is isomorphic to the group $\mathbb{R}^+$ of positive real numbers under multiplication.

3. Classify up to isomorphism all groups with 225 elements.

4. Do all four parts to receive full credit. Let G be a finite group.

   (a) What is a *subnormal series* for G?

   (b) What is a *composition series* for G?

   (c) What condition or conditions must G satisfy to be a *solvable group*?

   (d) Show that S_3 is solvable.

2 Rings

Do any two problems from this section.

1. Let $x^4 - 16$ be an element of the polynomial ring $E = \mathbb{Z}[x]$ and use the bar notation to denote passage to the quotient ring $\mathbb{Z}[x]/(x^4 - 16)$.

(a) Find a polynomial of degree ≤ 3 that is congruent to $7x^{13} - 11x^9 + 5x^5 - 2x^3 + 3$ modulo $(x^4 - 16)$.

(b) Prove that $\overline{x-2}$ and $\overline{x+2}$ are zero divisors in $\overline{E}$.

2. Prove that every Euclidean domain is a principal ideal domain (PID).

3. An integral domain D is said to be **Artinian** if for any descending chain of ideals

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq ...$$

of D, there is an integer n such that $I_i = I_n$ for all $i \geq n$. Prove that an integral domain D is Artinian if and only if it is a field. (Artinian rings are also referred to as rings satisfying the *Descending Chain Condition*.)

4. Prove the Third Isomorphism Theorem for Rings. That is prove that if R is a ring and I and J are ideals of R with $I \leq J$, then $R/J \approx (R/I)/(J/I)$.

3 Fields

Do two problems from this section with one of the problems being either 1 or 2.

1. Let $p(x) \in \mathbb{Q}[x]$ be a polynomial of degree 3.

   (a) Prove that if $p(x)$ is irreducible, then its Galois group is isomorphic to either A_3 or S_3.

   (b) Provide an example of a degree three polynomial $p(x) \in \mathbb{Q}[x]$ whose Galois group is not isomorphic to A_3 or S_3.

2. Let $q(x) = x^7 - 5 \in Q[x]$ and let S be a splitting field for $q(x)$.

   (a) Determine $[S : \mathbb{Q}]$, the dimension of S over $\mathbb{Q}$.

   (b) Determine two distinct subfields K and L of S such that K and L are properly contained in S and both properly contain $\mathbb{Q}$. Demonstrate that K and L are not equal and that they are indeed proper and properly contain $\mathbb{Q}$.

3. Let F be a finite field of characteristic p. Consider the Frobenius map $g : F \to F$, given by $g(x) = x^p$ for $x \in F$.

   (a) Prove that g is an automorphism of F.

   (b) Determine the set $\{\alpha : g(\alpha) = \alpha\}$, providing complete justification for your solution.

4. Let E be a finite extension of F. Prove that E is algebraic over F.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2004

1 Groups

Do any two questions from this section.

1. Let G be a finite group of order $4q^2$ where $q \geq 5$ is a prime number. Prove that there is a normal subgroup of order q^2.

2. Prove that an abelian group has a composition series if and only if it is finite.

3. Determine up to isomorphism all the abelian groups of order 1500.

2 Rings

Do any two questions from this section.

4. Let $Z[\sqrt{-3}] = \{m + n\sqrt{-3} : m, n \in Z\}$. Prove that $Z[\sqrt{-3}]$ is not a unique factorization domain. (Hint: You may want to use the function $N(a) = m^2 + 3n^2$ for all $a = m + n\sqrt{-3} \in Z[\sqrt{-3}]$.)

5. Recall that an element a from a ring R is nilpotent if $a^n = 0$ for some positive integer n. Let R be a ring with no nonzero nilpotent elements. Prove that if $f(x) \in R[x]$ is a zero divisor, then there exists $b \in R$ such that $b \cdot f(x) = 0$.

6. Prove the following result. In a commutative ring R with identity $1_R \neq 0$ an ideal P is prime if and only if R/P is an integral domain.

3 Fields

Do any two questions from this section.

7. Let Q be the field of rational numbers. In the field of complex numbers C, prove that the subfields $Q(i)$ and $Q(\sqrt{2})$ are isomorphic as vector spaces over Q, but not as fields.

8. Let $f(x) = x^5 - 6x + 2$
(a) Show that $f(x)$ is irreducible over Q, and that in C, it has exactly three real roots. (For the last part you need calculus.)
(ii) Deduce that if L is the splitting field of f over Q, $G = Gal(L/Q)$, when identified with a subgroup of S_5, contains a 5-cycle and a 2-cycle. (This implies that $G = S_5$, but you don't need to prove this.)

9. Prove or disprove the following:
(i) There are precisely p automorphisms of the field of order p.
(ii) All fields with 49 elements are isomorphic.
(iii) $Q(\sqrt{2}, \sqrt{3})$ is a simple extension of Q.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville
Spring 2003

1 Groups

Do any three problems out of the set below. Specify clearly which problems are you attempting.

1. Let G be a simple group of order 168. How many elements are there in G of order 7? What can you say about the number of elements of order 7 in G if G is not simple?

2. Show that a group with precisely two conjugacy classes is simple. Find an example of such a group.

3. Determine up to isomorphism all the abelian groups of order 108

4. Prove that if G is a finite group and H is a maximal normal subgroup then the quotient group G/H is simple. Prove that every finite group has a composition series.

5. Let G be a group of odd order, and let p be an odd prime that divides $|G|$. Prove that there are even number of elements of G of order p.

Do any four problems out of the sets **Rings** *and* **Fields** *below; do at least one problem in each set. Specify clearly which problems are you attempting.*

2 Rings

1. Consider the ideals $(3), (1+i), (2)$ in the ring $\mathbb{Z}[i]$ of the Gaussian integers.

   (a) Are these ideals maximal?

   (b) Are these ideals prime?

(c) Which of the quotient rings are fields?

(d) What are the characteristics of the fields above in 1c?

2. Let F be a field, and let S be the ring of all 2×2 matrices over F. Prove or disprove each statement:

   (a) The center $Z(S)$ of S is $\{\lambda I : \lambda \in F\}$, where I is the identity matrix.

   (b) $Z(S)$ is an ideal of S.

   (c) Let $A, B \in S$, then $(AB - BA)^2$ is in $Z(S)$.

3. (a) Prove that if D is a unique factorization domain, then so is the polynomial ring $D[x]$.

   (b) Prove or disprove that $\mathbb{Z}[x]$ is a unique factorization domain.

   (c) Decide if the following equations contradict the above statements:

$$x - 1 = (\sqrt{x} - 1)(\sqrt{x} + 1)$$

$$12x^3 + 4x^2 = 4x^2(3x + 1) = 2x(6x^2 + 2x)$$

3 Fields

1. Let K be a field and $f \in K[x]$ be an irreducible separable polynomial of degree 2. Determine the Galois group G of f.

2. Find the splitting field F of $f = x^4 + x^2 + 1$ over $\mathbb{Q}$ and calculate $[F : \mathbb{Q}]$.

3. Given $g = x^2 + x + 1 \in \mathbb{Z}_2[x]$, construct a field of four elements. Construct the addition and multiplication tables for this field.

Ph.D. Qualifying Examination in Algebra

Department of Mathematics
University of Louisville

17 th October 2003

The questions on this examination are presented in three sections - one section on **Groups**, *one on* **Rings** *and one on* **Fields**. *You should attempt at least two questions from each section. If you attempt three questions from one section you will be awarded the scores on your best two questions from that section.*

1 Groups

Do any two questions from this section.

1. Let G be an abelian group. For any integer $n > 0$ show that the map $\phi : x \mapsto x^n$ is a homomorphism of G into G. Characterize the kernel of ϕ. Show that if G is finite and n is relatively prime to the order of G then ϕ is an isomorphism. Deduce that in this case, for each element $g \in G$ there is a unique element $x \in G$ such that $g = x^n$.

2. For any group G the *center* $Z(G)$ of G is the set of elements of G that commute with all elements of G,

$$Z(G) = \{x \in G \mid xg = gx \ \forall \ g \in G\}.$$

   (a) Prove that if $G/Z(G)$ is cyclic then G is abelian.

   (b) Suppose that $G/Z(G)$ is abelian. Prove or disprove that G must also be abelian.

3. The Sylow theorems may be summarized as follows:

   If p^n is the largest power of a prime p dividing the order of a finite group G then G has a subgroup of order p^n. Any two such subgroups are conjugate in G and the number of such subgroups is conjugate to 1 *(mod p) and divides their common index.*

   (a) Let p and q be primes with $p > q$ and let G be a group of order pq. Then G has a $p-$Sylow subgroup P of order p and a $q-$Sylow subgroup Q of order q. Prove that $G = PQ$.

   (b) Show that every group of order 56 has a proper normal subgroup.

2 Rings

Do any two questions from this section.

1. (a) Let R be the ring given by defining new operations on the integers $\mathbf{Z}$ by letting $m \oplus n = m + n - 1$ and $m \otimes n = m + n - m.n$ where $+$ and $.$ are the usual operations of addition and multiplication on $\mathbf{Z}$. Define $\phi : \mathbf{Z} \rightarrow R$ by $\phi(n) = 1 - n$. Prove that ϕ is an isomorphism.

   (b) Note that ϕ maps the identity element 1 of $\mathbf{Z}(+, .)$ to the identity element 0 of $R(\oplus, \otimes)$. Prove that if θ is a homomorphism of a commutative ring with identity S to an integral doman D then θ maps the identity element of S to the identity element of D.

   (c) Show that a homomorphism of a ring V with identity into a ring W with identity does not necessarily map the identity element of V to the identity element of W.

2. Let R be a commutative ring with ideals I, J such that $I \subseteq J \subseteq R$. It is well known that J/I is an ideal of R/I.

   (a) Show that the factor ring $(R/I)/(J/I)$ is isomorphic to R/J. *Hint: Define a homomorphism from R/I onto R/J and apply the fundamental homomorphism theorem for rings.*

   (b) Using the result of Part (a), or otherwise, determine all prime ideals and all maximal ideals of $\mathbf{Z_n}$.

3. Let R be a ring with identity and let $x \in R$ have a right inverse y and a left inverse z. Prove that $y = z$.

   Suppose that K is a ring with identity 1 and let x be an element of K that has a right inverse y but has no left inverse. Prove that the function $\phi : z \mapsto y + zx - 1$ maps the set of right inverses of x into itself. Show that ϕ is one-to-one but not onto and deduce that if an element of a ring has more than one right inverse then it has an infinite number of right inverses.

3 Fields

Do any two questions from this section.

1. Let $K \subseteq E \subseteq F$ where E is a finite extension field of the field K and F is a finite extension field of the field E. It is well known that $[F : K] = [F : E][E : K]$.

   Using this result, or otherwise, prove that $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}] = 4$.

2. Construct a splitting field for the polynomial $x^3 - 2$ over $\mathbf{Q}$.

3. Define $\phi : GF(2^2) \to GF(2^2)$ by $\phi(x) = x^2$, for all $x \in GF(2^2)$.

   (a) Show that ϕ is an isomorphism.

   (b) Choose an irreducible polynomial $p(x)$ to represent $GF(2^2)$ as $\mathbf{Z_2}[x]/ < p(x) >$. For your choice of $p(x)$ give an explicit computation of $\phi(\beta)$ for each element β of $\mathbf{Z_2}[x]/ < p(x) >$.