You only need to choose **8** problems to answer.

1. Let G be a group and N, H be subgroups of G. Suppose that $N \triangleleft G$, $|H|$ is finite and $[G : N]$ is finite. If $[G : N]$ and $|H|$ are relatively prime, show that H is contained in N.

2. Let G be a group of order 2012.

   (a) Find the number of subgroups of order 503.

   (b) Find the number of elements of order 503.

3. Let R be a principal ideal domain and let J be a nonzero ideal of R. Show that J is a maximal ideal of R if and only if J is a prime ideal of R.

4. Let $\mathbb{Z}$ be the ring of integers and $\mathbb{Q}$ the additive group of rational numbers. Show that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ as groups.

5. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ and let $u = \sqrt[4]{2}$ be the positive real fourth root of 2. Suppose that $F \subseteq \mathbb{C}$ is a splitting field of $f(x)$ over $\mathbb{Q}$.

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

   (b) Is $\mathbb{Q}(u)$ normal over $\mathbb{Q}$?

   (c) Find the order of the Galois group $\mathrm{Aut}_{\mathbb{Q}} F$.

6. Let G be a group and let $n \in \mathbb{N}$. Suppose H is the only subgroup of G of order n. Prove that H is a normal subgroup of G.

7. Let G be a finitely generated abelian group in which no element, except 0, has finite order. Prove that G is a free abelian group.

8. Let I be an ideal in a commutative ring R. Let $\mathrm{Rad}I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}$. Prove that $\mathrm{Rad}I$ is an ideal of R.

9. Let R be a ring with identity and suppose $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $gf = 1_A$. Prove that $B = \mathrm{Im}f \oplus \mathrm{Ker}g$, i.e., $B = \mathrm{Im}f + \mathrm{Ker}g$ and $\mathrm{Im}f \cap \mathrm{Ker}g = 0$.

10. Let F be an extension field of a field K and let $u, v \in F$ be algebraic over K. Suppose the irreducible polynomials of u and v over K have degree m and n respectively.

    (a) Prove that $[K(u, v) : K] \leq mn$.

    (b) If we further assume that m and n are relatively prime, prove that $[K(u, v) : K] = mn$.

國立台灣師範大學數學系博士班資格考試

科目：代數

2013 年 4 月 30 日

1. (16 pts) Let $f : G \to H$ be a group homomorphism.

   (a) Suppose $a \in G$ has finite order n. Prove that $f(a) \in H$ has finite order m with $m \mid n$.

   (b) Suppose G is cyclic and f is onto. Prove that H is also cyclic.

2. (18 pts) Let G be a finite group with $|G| = p^n q$ ($n \geq 1$) where p, q are primes such that $p > q$.

   (a) Show that G is not a simple group.

   (b) Assume that G acts on a set X with $|X| = q$. Show that this action must be either trivial or transitive. (Recall that G acts on X trivially if $g \cdot x = x$ for all $x \in X$ and all $g \in G$ and the action is transitive if for any $x_1, x_2 \in X$ there exists a $g \in G$ such that $x_2 = g \cdot x_1$.)

3. Let R be a commutative ring with identity 1.

   (a) (10 pts) Let M be an ideal of R. Prove that M is a maximal ideal if and only if for every $r \in R \setminus M$, there exists $x \in R$ such that $1 - rx \in M$.

   (b) (12 pts) Let J be the intersection of all maximal ideals of R and let $U(R)$ be the group of units of R. Prove that $1 + J = \{1 + x \mid x \in J\}$ is a subgroup of $U(R)$.

4. (12 pts) Let R be a principal ideal domain and let B be a submodule of a unitary R-module A. Suppose A can be generated by n elements with $n < \infty$. Prove that B can be generated by m elements with $m \leq n$.

5. (14 pts)

   (a) Construct a finite field of 125 elements. Does there also exist a finite field of 120 elements? (You need to explain your answer.)

   (b) Let $\mathbb{E}$ be a finite extension of a finite field $\mathbb{F}$. Show that $\mathbb{E}$ must be a Galois extension of $\mathbb{F}$ such that the Galois group $\mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$ of $\mathbb{E}$ over $\mathbb{F}$ is a cyclic group.

6. (18 pts) Let $K = \mathbb{C}(t)$ be the rational function field in the variable t over the complex numbers $\mathbb{C}$. Let n be a positive integer and let $f(x) = x^n + t \in K[x]$.

   (a) Prove or disprove that $f(x)$ is irreducible over K.

   (b) Let $\overline{K}$ be an algebraic closure of K and let $u \in \overline{K}$ be a zero of $f(x)$. Let $L = K(u)$. Show that L is Galois over K and that for every divisor d of n there exists a unique intermediate subfield M of L (i.e. $K \subseteq M \subseteq L$) such that $[M : K] = d$.

Algebra Qualifying Exam

Fall 2013

- Please choose **Five** of the following six questions to answer.

1. (a) Let G be a group and suppose that H is a normal subgroup of G. If H is cyclic, prove that every subgroup of H is normal in G.

   (b) Find a finite group G which has subgroups H and K satisfying the following conditions:

      i. H is a normal subgroup of K.
      ii. K is a normal subgroup of G.
      iii. H is not a normal subgroup of G.

2. Let G be a group of order 2013.

   (a) Show that G has a normal subgroup of order 11.

   (b) Show that G has a subgroup of order 33 and such a subgroup is abelian.

3. Let R be a ring with identity 1. Recall that an ideal P in R is said to be prime if $P \neq R$ and for any ideals A, B in R, we have $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$. Now suppose that I is an ideal of R and $I \neq R$. Show that the following are equivalent.

   (a) I is a prime ideal of R.

   (b) If $r, s \in R$ such that $rRs \subseteq I$, then $r \in I$ or $s \in I$.

4. Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module.

   (a) Prove that any two distinct elements $\alpha, \beta \in \mathbb{Q} \setminus \{0\}$ are linearly dependent over $\mathbb{Z}$.

   (b) Prove that no element in $\mathbb{Q}$ can generate $\mathbb{Q}$ over $\mathbb{Z}$, i.e., for any $q \in \mathbb{Q}$, $\langle q \rangle \subsetneq \mathbb{Q}$ where $\langle q \rangle = \{nq \mid n \in \mathbb{Z}\}$.

   (c) Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

5. (a) Prove that $x^3 + 2x + 1 \in \mathbb{Z}_7[x]$ is an irreducible polynomial in $\mathbb{Z}_7[x]$.

   (b) Construct a field of 27 elements.

   (c) Is there a field of 2013 elements? Explain your answer.

6. (a) Let $u \in \mathbb{C}$ be a zero of the polynomial $x^4 + 2x + 2$. Please write $\frac{1}{u}$ as a polynomial of u, i.e., find a polynomial $f(x) \in \mathbb{Q}[x]$ such that $\frac{1}{u} = f(u)$.

   (b) Let K be an algebraic extension field of a field F and let D be an integral domain such that $F \subseteq D \subseteq K$. Prove that D is indeed a field.

Algebra Qualifying Exam
Spring 2014

1. Show that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. (8 pts)

2. (a) Define the characteristic of a ring. (4 pts)

   (b) Let F be a field. Show that the characteristic of F is either 0 or a prime p. (8 pts)

   (c) Let F be a finite field of prime characteristic p. Show that F has p^n elements for some positive integer n. (8 pts)

3. Show that a group of order p^2q, where p and q are distinct primes, contains a normal Sylow subgroup. (12 pts)

4. Let $R = \mathbb{Z}/7\mathbb{Z}$.

   (a) Show that the polynomial ring $R[x]$ is a principal ideal domain. (8 pts)

   (b) Find all prime ideals of the ring $R[x]/\langle x^2 - 2 \rangle$. (8 pts)

5. Let $F = \mathbb{Q}(\sqrt{3}, \sqrt{11})$.

   (a) Find the Galois group $\text{Aut}_\mathbb{Q} F$. (6 pts)

   (b) Find the corresponding intermediate fields of F. (6 pts)

   (c) Find all normal extensions of $\mathbb{Q}$ in F. (6 pts)

6. Show that any ring with identity is isomorphic to a ring of endomorphisms of an abelian group. (8 pts)

7. Let R be a commutative ring with identity and let M be a finitely generated R-module. Let $f : M \to R^n$ be a surjective R-module homomorphism. Show that $\text{Ker } f$ is finitely generated. (8 pts)

8. Let G be a group and let $C(G) = \{a \in G \mid ga = ag, \ \forall g \in G\}$.

   (a) Prove that $C(G)$ is a normal subgroup of G. (8 pts)

   (b) Prove that if $G/C(G)$ is cyclic then G is abelian. (8 pts)

9. Let R be a commutative ring with identity and let $I = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{N}\}$.

   (a) Prove that I is an ideal of R. (6 pts)

   (b) Prove that every prime ideal of R contains I. (6 pts)

10. Let R be a ring with identity and let M be an R-module. Suppose $f : M \to M$ is an R-module homomorphism such that $ff = f$. Prove that $M = \text{Ker } f \oplus \text{Im } f$. (8 pts)

11. Suppose R is a commutative ring with identity such that every submodule of every free R-module is free. Prove that R is a principal ideal domain. (12 pts)

12. Prove that no finite field is algebraically closed. (8 pts)

Algebra Qualifying Exam

Fall 2015

1. Let G be an abelian group and let $a, b \in G$. Suppose the order of a is m and the order of b is n and $\gcd(m, n) = 1$. Prove that the order of ab is mn. (10 pts)

2. Let G be a group of order 63.

   (a) Prove that G is not simple. (6 pts)

   (b) Prove that G contains a subgroup of order 21. (8 pts)

3. Prove that $\mathbb{Q}$ is not a free abelian group, i.e., not a free $\mathbb{Z}$-module. (12 pts)

4. Let R and S be commutative rings with $1 \neq 0$ and let $f : R \to S$ be a homomorphism of commutative rings. Suppose J is an ideal of S.

   (a) Prove that $f^{-1}(J) = \{a \in R \mid f(a) \in J\}$ is an ideal of R. (5 pts)

   (b) Assume $f(1_R) = 1_S$ and J is a prime ideal of S. Prove that $f^{-1}(J)$ is a prime ideal of R. (7 pts)

5. Let R be a commutative ring with identity $1 \neq 0$ and let J be the intersection of all maximal ideals of R. Consider an element $x \in R$.

   (a) Suppose $x \in J$. Prove that $1 + x$ is a unit in R. (6 pts)

   (b) Suppose $x \notin J$. Prove that there exists an element $r \in R$ such that $1 - rx$ is not a unit in R. (8 pts)

6. Let R be an integral domain and let A be a unitary R-module. Prove that

$$T(A) = \big\{a \in A \mid ra = 0 \text{ for some } \textit{nonzero } r \in R\big\}$$

   is a submodule of A. (8 pts)

7. Let R be a principal ideal domain and let A be a finitely generated unitary R-module. Suppose A can be generated by n elements and let B be a submodule of A. Prove that B can be generated by m elements with $m \leq n$. (10 pts)

8. Prove that $\mathbb{Q}[i]$ and $\mathbb{Q}[\sqrt{2}]$ are isomorphic as $\mathbb{Q}$-vector spaces but they are not isomorphic as fields. (8 pts)

9. Let $K \leq E \leq F$ be fields and suppose F is a cyclic extension of K, *i.e., F is algebraic and Galois over K and the Galois group* $\mathrm{Aut}_K F$ *is cyclic.* Prove that F is a cyclic extension of E and E is a cyclic extension of K. (12 pts)

Algebra Qualifying Exam
Spring 2016

1. (a) Please state Lagrange's Theorem. (**4 pts**)

   (b) Please state Cauchy's Theorem. (**4 pts**)

   (c) Please state the First Isomorphism Theorem. (**4 pts**)

2. Let G_1 and G_2 be groups. Suppose N_1 is a normal subgroup of G_1 and N_2 is a normal subgroup of G_2. Prove that $N_1 \times N_2$ is a normal subgroup of $G_1 \times G_2$ and

$$\left(G_1 \times G_2\right)/\left(N_1 \times N_2\right) \simeq G_1/N_1 \times G_2/N_2. \qquad \text{(12 pts)}$$

3. Let $p > q$ be two prime numbers and suppose G is a group of order $p^2 q$.

   (a) Prove that G is not simple. (**7 pts**)

   (b) Prove that G contains at least three cyclic subgroups. (**7 pts**)

4. Suppose R is a ring such that $r^2 = r$ for all $r \in R$. Prove that R is commutative. (**8 pts**)

5. Let R be a commutative rings with $1 \neq 0$ and let $J = \{r \in R \mid r^n = 0 \text{ for some } n \in \mathbb{N}\}$.

   (a) Prove that J is an ideal of R. (**7 pts**)

   (b) Suppose P is a prime ideal of R. Prove that $J \subseteq P$. (**7 pts**)

6. (a) Let R be a commutative ring and let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a sequence of R-modules and R-module homomorphisms. What does it mean that this sequence is exact? (**7 pts**)

   (b) Suppose $0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \xrightarrow{f_3} V_4 \xrightarrow{f_4} V_5 \to 0$ is an exact sequence of $\mathbb{Q}$-vector spaces and linear transformations. Prove that

$$\dim V_1 + \dim V_3 + \dim V_5 = \dim V_2 + \dim V_4. \qquad \text{(7 pts)}$$

7. Let F be an algebraically closed field. Prove that $|F| = \infty$. (**8 pts**)

8. Let F be an extension field of a field K.

   (a) What does it mean that F is normal over K? (**6 pts**)

   (b) Is $\mathbb{Q}(\sqrt[4]{2})$ normal over $\mathbb{Q}$? Please explain your answer. (**6 pts**)

   (c) Is $\mathbb{Q}(\sqrt[4]{2}, i)$ normal over $\mathbb{Q}$? Please explain your answer. (**6 pts**)

Algebra Qualifying Exam
Fall 2018

1. Let G be a simple group of order 168.

   (a) (8 pts) Find the number of elements of order 7 in G.

   (b) (6 pts) Suppose that P is a Sylow 7-subgroup of G and $\mathbf{N}_G(P)$ is the normalizer of P in G. Find the order of $\mathbf{N}_G(P)$.

   (c) (8 pts) Prove that G has no element of order 14.

2. Let G be a group. Recall that for each $g \in G$, a map $\theta_g : G \to G$ given by $\theta_g(x) = gxg^{-1}$ is called an inner automorphism of G. Let $\mathrm{Inn}(G)$ be the group of all inner automorphisms of G.

   (a) (8 pts) Let $\mathbf{Z}(G)$ be the center of G. Prove that $G/\mathbf{Z}(G) \cong \mathrm{Inn}(G)$.

   (b) (8 pts) Let S_4 be the symmetric group of degree 4. Show that $S_4 \cong \mathrm{Inn}(S_4)$.

3. (10 pts) If R is a principal ideal domain, is it always true that the polynomial ring $R[x]$ is a principal ideal domain? Justify your answer.

4. (10 pts) Let R be a ring with 1 and let M be a unitary R-module. Suppose $f : M \to M$ is an R-module homomorphism such that $ff = f$. Prove that $M = \mathrm{Ker} f \oplus \mathrm{Im} f$.

5. (10 pts) Let R be a principal ideal domain and let A be a finitely generated unitary R-module. Suppose A can be generated by n elements and let B be a submodule of A. Prove that B can be generated by m elements with $m \leq n$.

6. Let $\mathbb{Q}$ be the field of rational numbers and let $\mathbb{C}$ be the field of complex numbers. Let $f(x) = x^4 - 5$ in $\mathbb{Q}[x]$. Suppose that $E \subseteq \mathbb{C}$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

   (a) (8 pts) Show that $f(x)$ is irreducible over $\mathbb{Q}$.

   (b) (8 pts) Let $\alpha = \sqrt[4]{5}$ be the unique positive real root of $x^4 - 5$. Let $i = \sqrt{-1}$ in $\mathbb{C}$. Show that $E = \mathbb{Q}(\alpha, i)$.

   (c) (8 pts) Determine $[E : \mathbb{Q}]$.

   (d) (8 pts) Let $K = \mathbb{Q}(\sqrt{5})$. Determine the Galois group $\mathrm{Aut}_K E$.

Algebra Qualifying Exam.
Spring 2019

1. (a) Let F be a field and let $F^* = F - \{0\}$ be the multiplicative group of F. Show that every finite subgroup of F^* is cyclic. (10 pts)

   (b) Describe all finite subgroups of $C^* = C - \{0\}$, where C is the field of complex numbers. (5 pts)

2. (a) Let $f(x) \in Q[x]$ with degree n. Show that if $f(x)$ is irreducible over Q, then the Galois group G_f of $f(x)$ over Q is a transitive subgroup of S_n. (8 pts)

   (b) For $f(x) = x^5 - 6x + 3$, show that the Galois group G_f of $f(x)$ over Q is S_5. (7 pts)

3. Let R be a ring and J be an ideal of R.

   (a) Show that $M_{2 \times 2}(J)$ is an ideal of $M_{2 \times 2}(R)$. (5 pts)

   (b) Show that every ideal of $M_{2 \times 2}(R)$ is of the form $M_{2 \times 2}(J)$, where J is an ideal of R. (12 pts)

4. (a) Find the ideal consists of all the nilpotent elements of the ring Z_{12}. (5 pts)

   (b) For a commutative ring R with 1, show that the ideal of R which consists of all the nilpotent elements of R is equal to the intersection of all prime ideals of R. (12 pts)

5. Let G be a nonabelian group of order 12 which has a normal subgroup of order 4.

   (a) Show that G has 4 Sylow 3-subgroups. (6 pts)

   (b) Show that G is isomorphic to the Alternating group A_4. (10pts)

6. Let G be a finite group and let p be the smallest prime divisor of the order of G. Show that every subgroup H of G of index p is a normal subgroup of G. (10 pts)

7. Let R be a ring with identity. Suppose M_1, M_2 and N are submodules of an R-module M such that M_1 is a submodule of M_2. Show that there is an exact sequence of R-modules

   $$0 \rightarrow (M_2 \cap N)/(M_1 \cap N) \rightarrow M_2/M_1 \rightarrow (M_2 + N)/(M_1 + N) \rightarrow 0.$$ (10 pts)

Notations : Q : The field of rational numbers. $M_{2 \times 2}(R)$: 2×2 matrix ring over R.

Algebra Qualifying Exam

Fall 2019

1. Let S_n be the symmetric group of degree n. Let A_n be the alternating group of degree n.

   (a) Find the number of elements of order 3 in S_5. (6 pts)

   (b) Let P be a Sylow 3-subgroup of S_5. Let N be the normalizer of P in S_5. Find the order of N. (6 pts)

   (c) Find the number of Sylow 2-subgroups of S_4. (6 pts)

   (d) Show that S_4 is solvable. (8 pts)

   (e) Is it true that every finite group is isomorphic to a subgroup of A_n for some positive integer n? (8 pts)

2. Let R be a ring with identity. An element r in R is called nilpotent if $r^n = 0$ for some positive integer n. An ideal I of R is called nil if every element of I is nilpotent. Suppose that R is not commutative. For any two nil ideals J, K of R, is it always true that $J + K$ is nil? (10 pts)

3. If R is a unique factorization domain, show that every nonzero prime ideal in R contains a nonzero principal ideal that is prime. (10 pts)

4. Let R be a ring with identity. Let A, B be R-modules. Let 1_A be the identity function on A. Suppose $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $gf = 1_A$. Prove that $B = \operatorname{Im} f \oplus \operatorname{Ker} g$. (10 pts)

5. Let K be a field and let $f(x)$ be a polynomial in $K[x]$ of positive degree. Let E be a splitting field of $f(x)$ over K and let $G = \operatorname{Aut}_K(E)$ be the Galois group of f. Let $\Lambda = \{\, \alpha \in E \mid f(\alpha) = 0 \,\}$. We use $\operatorname{Sym}(\Lambda)$ to denote the group of all bijections on Λ under the operation of function composition.

   (a) Show that G is isomorphic to a subgroup of $\operatorname{Sym}(\Lambda)$. (8 pts)

   (b) If $f(x)$ is irreducible separable over K and $f(x)$ has degree n, show that n divides $|G|$ and G is isomorphic to a transitive subgroup of S_n. (10 pts)

6. Let $f(x) = x^4 + 2x^2 + 4 \in \mathbb{Q}[x]$.

   (a) Show that $f(x)$ is irreducible over $\mathbb{Q}$. (8 pts)

   (b) Let E be the splitting field of $f(x)$ over $\mathbb{Q}$ in $\mathbb{C}$. Determine the Galois group $\operatorname{Aut}_{\mathbb{Q}} E$ of $f(x)$ over $\mathbb{Q}$. (10 pts)

Algebra Qualifying Exam
Spring 2020

- Let $\mathbb{Q}$ be the field of rational numbers.

- Let $\mathbb{R}$ be the field of real numbers.

1. (20 pts) Let G be a group. Let G' be the commutator subgroup of G. Let G'' be the commutator subgroup of G'.

   (a) If H is a subgroup of G, show that $\mathrm{N}_G(H)/\mathrm{C}_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

   (b) If G'' is cyclic, show that G'' is contained in the center of G'.

2. (10 pts) Let D be the dihedral group of order $2n$. Write $2n = 2^k m$ where k, m are positive integers and m is odd. Show that D has exactly m Sylow 2-subgroups.

3. (20 pts) Let R be a ring with 1 and let $\mathrm{M}_2(R)$ be the ring of 2×2 matrices over R. If I is an ideal of R, we know that $\mathrm{M}_2(I)$ is an ideal of $\mathrm{M}_2(R)$.

   (a) Show that if J is an ideal of $\mathrm{M}_2(R)$, then $J = \mathrm{M}_2(I)$ for some ideal I of R.

   (b) If L is a maximal ideal of R, is it always true that $\mathrm{M}_2(L)$ is a maximal ideal of $\mathrm{M}_2(R)$?

4. (20 pts) Let R be a ring and let

$$
\begin{array}{ccccccc}
A_1 & \xrightarrow{f} & A_2 & \xrightarrow{g} & A_3 & \xrightarrow{h} & A_4 \\
\downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} & & \downarrow{\delta} \\
B_1 & \xrightarrow{f'} & B_2 & \xrightarrow{g'} & B_3 & \xrightarrow{h'} & B_4
\end{array}
$$

   be a commutative diagram of R-modules and R-module homomorphisms with exact rows. Suppose that α is an epimorphism and δ is a monomorphism.

   (a) If β is a monomorphism, show that γ is a monomorphism.

   (b) If γ is an epimorphism, show that β is an epimorphism.

5. (15 pts)

   (a) Suppose $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ and $r \in \mathbb{R}$. If $r > 0$, show that $\sigma(r) > 0$.

   (b) Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ is the trivial group.

6. (15 pts) Let $f(x) = (x^3 - 2)(x^2 + 3) \in \mathbb{Q}[x]$. Let K be a splitting field of $f(x)$ over $\mathbb{Q}$. Determine the Galois group $\mathrm{Aut}_{\mathbb{Q}}(K)$ of $f(x)$.

Algebra Qualifying Exam

Fall 2020

- Let $\mathbb{Q}$ be the field of rational numbers.

1. (15 pts) Let A_n be the alternating group of degree n. Let D_n be the dihedral group of order $2n$. Determine if the following statements are true. Justify your answer.

   (a) Any finite group is isomorphic to a subgroup of A_n for some positive integer n.

   (b) Any finite group is isomorphic to a subgroup of D_n for some positive integer n.

2. (20 pts) Let G be a finite group and let p be a prime. For convenience, we use $n_p(G)$ to denote the number of Sylow p-subgroups of G. Suppose that H is a group and there is a surjective group homomorphism $\varphi : G \to H$.

   (a) If P is a Sylow p-subgroup of G, show that $\varphi(P)$ is a Sylow p-subgroup of H.

   (b) Prove that $n_p(H) \leqslant n_p(G)$.

3. (20 pts)

   (a) Let $c \in F$, where F is a field of characteristic $p > 0$. Prove that $x^p - x - c$ is irreducible in $F[x]$ if and only if $x^p - x - c$ has no root in F.

   (b) Find an element $c \in \mathbb{Q}$ such that the polynomial $f(x) = x^5 - x - c$ has no root in $\mathbb{Q}$ and $f(x)$ is reducible in $\mathbb{Q}[x]$.

4. (15 pts) Let R be a ring with 1 and let

$$
\begin{array}{ccccc}
A_1 & \xrightarrow{f} & A_2 & \xrightarrow{g} & A_3 \\
\downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} \\
B_1 & \xrightarrow{f'} & B_2 & \xrightarrow{g'} & B_3
\end{array}
$$

be a commutative diagram of R-modules and R-module homomorphisms with exact rows. Suppose that α and g are epimorphisms and β is a monomorphism. Prove that γ is a monomorphism.

5. (15 pts) Construct a finite field of order 125.

6. (15 pts) Let $f(x) = x^3 - 2x + 2 \in \mathbb{Q}[x]$. Let K be a splitting field of $f(x)$ over $\mathbb{Q}$. Determine the Galois group $\text{Aut}_{\mathbb{Q}}(K)$ of $f(x)$.

Modern Algebra Qualifying Examination
Spring 2021

April 27, 2021

1. For a group G, let G' denote its commutator subgroup. Assume that G is a simple group.

   (a) (5 %) Show that if G' is not the trivial subgroup of G then $G' = G$. Classify all simple groups G such that G' is the trivial subgroup. Give an example of non-trivial simple group G such that $G' = G$.

   (b) (5 %) Let $\varphi : G \to G$ be a surjective endomorphism of G. Show that φ is an automorphism of G.

2. Let A be an abelian group with group law written additively and, for every integer $m \geq 1$, let
$$A_m := \{a \in A \ : \ ma = \mathcal{O}\}$$
be the subgroup of elements of order dividing m where $\mathcal{O}$ denotes the zero element of A.

   (a) (10 %) Suppose that A has order M^2, and further assume that for every integer m dividing M, the subgroup A_m has order m^2. Prove that A is the direct product of two cyclic group of order M.

   (b) (6 %) Find an example of a non-abelian group G and an integer m such that the set $G_m := \{g \in G \ : \ g^m = e\}$ is not a subgroup of G.

3. Let S_n denote the group of permutations on the set $\{1, 2, \ldots, n\}$ of n letters. In the following, we fix a prime number p.

   (a) (5 %) Give a p-Sylow subgroup of S_p.

   (b) (12 %) Determine the number of p-Sylow subgroups of S_p. (If you don't know how to do this for general prime p, try to find the answer for $p = 5$ and make a conjecture about the answer for general prime p).

4. Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module.

   (a) (5 %) Prove that any two distinct elements $\alpha, \beta \in \mathbb{Q} \setminus \{0\}$ are linearly dependent over $\mathbb{Z}$.

   (b) (5 %) Prove that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

   (c) (10 %) Prove that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module.

5. (12 %) Let R be a commutative ring with identity 1 and let I be an ideal of R. Suppose that $I \subseteq P_1 \cup \cdots \cup P_n$ for some prime ideals $P_1, \ldots, P_n$. Prove that $I \subseteq P_i$ for some i.

6. Let $f(x) = x^5 - 5 \in \mathbb{Q}[x]$ and let $\alpha = \sqrt[5]{5}$ be the unique positive real root of $f(x)$. Suppose that $E \subset \mathbb{C}$ is the splitting field (in $\mathbb{C}$) of $f(x)$ over $\mathbb{Q}$ where $\mathbb{C}$ denotes the field of complex numbers.

(a) (10 %) Let $\phi : \mathbb{Q}[x] \to \mathbb{C}$ be the ring homomorphism defined by $\phi(f(x)) = f(\alpha)$ for $f(x) \in \mathbb{Q}[x]$. Show that the image F of ϕ is a subfield of E. Is F equal to E? Why?

(b) (5 %) Determine $[E : F]$ and $[F : \mathbb{Q}]$.

(c) (10 %) Is it true that E is a Galois extension of $\mathbb{Q}$? If your answer is yes, compute the Galois group $\mathrm{Gal}(E/\mathbb{Q})$; otherwise, explain why $E/\mathbb{Q}$ is not a Galois extension.

⊚ *Among the following 18 problems, choose at most **13** problems to answer. If you answer more than 13 problems, only the first 13 problems will be graded.*

1. (a) Suppose $\varphi : S_4 \to S_3$ is an epimorphism. Find $\operatorname{Ker} \varphi$ and prove your answer. (8%)

(b) Prove that there is no epimorphism $\varphi : S_5 \to S_4$. (8%)

2. (a) Prove that the additive group $\mathbb{Q}$ is not finitely generated. (8%)

(b) Prove that $\mathbb{Q}$ is not a free abelian group. (8%)

3. (a) Let G be a group of order 2022. Prove that G contains a normal Sylow subgroup. (8%)

(b) Let G be a group of order 56. Prove that G contains a normal Sylow subgroup. (8%)

(c) Let G be a simple group of order 168. How many elements of order 7 are there in G? Please explain your answer. (8%)

4. Let F be a field.

(a) Prove that (x) is a maximal ideal in $F[x]$. (8%)

(b) Prove that $F[x]$ has more than one maximal ideals. (8%)

5. Suppose $f : A \to B$ and $g : B \to A$ are R-module homomorphisms such that $gf = 1_A$.

(a) Prove that $B = \operatorname{Im} f + \operatorname{Ker} g$. (8%)

(b) Prove that $\operatorname{Im} f \cap \operatorname{Ker} g = 0$. (8%)

6. Let F be an extension field of a field K.

(a) Let $u, v \in F$. Suppose v is algebraic over $K(u)$ and v is transcendental over K. Prove that u is transcendental over K. (8%)

(b) Suppose $u \in F$ is algebraic of odd degree over K. Prove that $K(u) = K(u^2)$. (8%)

(c) Suppose F is algebraic over K and D is an integral domain such that $K \subseteq D \subseteq F$. Prove that D is indeed a field. (8%)

7. Consider the subfields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ of $\mathbb{C}$.

(a) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces over $\mathbb{Q}$. (8%)

(b) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are not isomorphic as fields. (8%)

8. (a) Please construct a field of order 8. (8%)

(b) Please describe the Galois group of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$. (8%)

1. (10 pts) Prove that $\mathbb{Q}$ is not a free abelian group.

2. (10 pts) Let G be a group and let $C(G)$ denote the center of G. For each $g \in G$, a map $\theta_g : G \to G$ given by $\theta_g(x) = gxg^{-1}$ is called an inner automorphism of G. Let $\text{Inn}(G)$ be the group of all inner automorphisms of G. Prove that $G/C(G) \simeq \text{Inn}(G)$.

3. (8 pts) Let G be a group of order 2024. Prove that G contains a normal Sylow subgroup.

4. (10 pts) Let R and S be commutative rings with $1 \neq 0$. Suppose $f : R \to S$ is a homomorphism of rings such that $f(1_R) = 1_S$. Suppose J is a prime ideal of S. Prove that $f^{-1}(J) = \{r \in R \mid f(r) \in J\}$ is a prime ideal of R.

5. (12 pts) Suppose $f : A \to A$ is an R-module homomorphism such that $ff = f$. Prove that $A = \text{Ker } f + \text{Im } f$ and $\text{Ker } f \cap \text{Im } f = 0$.

6. Let F be an extension field of a field K.

(a) (8 pts) Suppose $u \in F$ is algebraic of odd degree over K. Prove that $K(u) = K(u^2)$.

(b) (8 pts) Suppose F is algebraic over K and D is an integral domain with $K \subseteq D \subseteq F$. Prove that D is indeed a field.

7. Consider the subfields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ of $\mathbb{C}$.

(a) (6 pts) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces over $\mathbb{Q}$.

(b) (6 pts) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are not isomorphic as fields.

8. (8 pts) Let F be a finite field. Prove that F is not algebraically closed.

9. Let $\text{Aut}_{\mathbb{Q}}(\mathbb{R})$ be the group of $\mathbb{Q}$-automorphisms of $\mathbb{R}$.

(a) (4 pts) Suppose $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{R})$ and $r \in \mathbb{R}$. If $r > 0$, prove that $\sigma(r) > 0$.

(b) (10 pts) Prove that $\text{Aut}_{\mathbb{Q}}(\mathbb{R})$ is the trivial group.

ALGEBRA QUALIFYING EXAMINATION
FALL, 2024

(1) (6 %) How many **non-isomorphic abelian groups** of order 2024 are there? You need to explain your answer.

(2) Let G be a finite group of order $|G| = p^n q$ $(n \geq 1)$ where p and q are prime numbers such that $p > q$.

   (a) (5 %) Show that G is not a simple group.

   (b) (7 %) Assume that G acts on a finite set X with $|X| = q$ elements. Show that the action must be either trivial or transitive. (Recall that G acts on X trivially if $g \cdot x = x$ for all $x \in X$ and all $g \in G$ and the action is transitive if for any $x_1, x_2 \in X$ there exists a $g \in G$ such that $x_2 = g \cdot x_1$)

(3) Let S_n denote the group of permutations on the set $\{1, 2, \ldots, n\}$ of n letters. In the following, we fix an odd prime number p.

   (a) (7 %) Determine the number of the Sylow p-subgroups of S_p. (*Hint.* Determine the number of elements of order p in S_p)

   (b) (8 %) Determine the number of the Sylow p-subgroups of S_{p+1} and the number of the Sylow p-subgroups of S_{p+2} respectively.

(4) (a) (5 %) Let R be a commutative ring with identity 1. Let J be the intersection of all maximal ideal of R and let $U(R)$ be the group of units of R. Prove that $1 + J := \{1 + x \mid x \in J\}$ is a subgroup of $U(R)$.

   (b) (7 %) Show that in a principal ideal domain R, a non-zero ideal is a prime ideal of R if and only if it is a maximal ideal of R.

(5) Let $\mathbb{A} = \mathbb{Z}[x]$, the polynomial ring over the ring of integers.

   (a) (6 %) Is $\mathbb{A}$ a principal ideal domain? If your answer is yes, give a proof; otherwise, explain your answer by giving an ideal which is not principal in $\mathbb{A}$.

   (b) (9 %) Let p be a prime number. Show that the ideal $\langle p \rangle := p\mathbb{A}$ generated by p is a prime ideal in $\mathbb{A}$.

   (c) (10 %) Show that the ideal
   $$\mathfrak{a} = \langle 7, x^2 + 1 \rangle = \{7 \cdot s(x) + (x^2 + 1) \cdot t(x) \mid s(x), t(x) \in \mathbb{A}\}$$
   generated by 7 and $x^2 + 1$ is a maximal ideal in $\mathbb{A}$; while the ideal $\mathfrak{b} = \langle 5, x^2 + 1 \rangle$ generated by 5 and $x^2 + 1$ is not maximal in $\mathbb{A}$.

(6) Let $\mathbb{Q}[x]$ denote the polynomial ring with coefficients in $\mathbb{Q}$. Define the map
$$\phi : \mathbb{Q}[x] \to \mathbb{R} \text{ by } \phi(f) = f(\sqrt{2} - \sqrt{3}) \text{ for } f(x) \in \mathbb{Q}[x].$$

(a) (5 %) Verify that ϕ is a ring homomorphism from $\mathbb{Q}[x]$ to $\mathbb{R}$.

(b) (10 %) Show that the image of ϕ is a subfield F of $\mathbb{R}$ containing $\mathbb{Q}$ and determine the degree $[F : \mathbb{Q}]$ of F over $\mathbb{Q}$.

(7) Let $\mathbb{F}_q$ denote a finite field with q elements. Let $P(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $d \geq 1$ over $\mathbb{F}_q$.

(a) (10 %) Let $E = \mathbb{F}_q[x]/\langle P(x) \rangle$ be the quotient of $\mathbb{F}_q[x]$ by the ideal $\langle P(x) \rangle$ generated by $P(x)$. Prove that E is a cyclic Galois extension of $\mathbb{F}_q$ and compute the Galois group $\text{Gal}(E/\mathbb{F}_q)$ of E over $\mathbb{F}_q$. How many elements does E have? (**Recall: a Galois extension E/F is called a cyclic Galois extension if its Galois group $\text{Gal}(E/F)$ is a cyclic group**)

(b) (5 %) Construct a finite field with $q = 16$ elements.

Algebra Qualifying Exam

Spring 2025

- Let $\mathbb{Q}$ be the field of rational numbers and let $\mathbb{C}$ be the field of complex numbers.

1. (28 pts) Let S_n be the symmetric group on the set $\{1, 2, \ldots, n\}$. Now consider the group $G = S_6$.

    (a) Let $x = (123)(456) \in G$. The conjugacy class of x in G is defined to be the set $x^G = \{g^{-1}xg \mid g \in G\}$. Determine the number of elements in x^G.

    (b) For any Sylow 3-subgroup P of G, prove that P is generated by two disjoint 3-cycles.

    (c) Determine the number of Sylow 3-subgroups of G.

2. (10 pts) Let G be a group of order pn with $p > n$ where p is a prime and n is a positive integer. If H is a subgroup of G of order p, prove that H is normal in G.

3. (10 pts) Let R be an integral domain and let S, T be two ideals of R. Define the set $S * T = \{st \mid s \in S, t \in T\}$. Now, if $a, b \in S * T$, is it always true that $a + b \in S * T$? If you think it is true, prove it; if your answer is no, give a counterexample.

4. (10 pts) Let R be a unique factorization domain and d a nonzero element of R. Prove that there are only a finite number of distinct principal ideals that contain the ideal (d).

5. (16 pts) Let R be a ring with 1 and let

$$
\begin{array}{ccccc}
A_1 & \xrightarrow{f} & A_2 & \xrightarrow{g} & A_3 \\
\downarrow{\alpha} & & \downarrow{\beta} & & \downarrow{\gamma} \\
B_1 & \xrightarrow{f'} & B_2 & \xrightarrow{g'} & B_3
\end{array}
$$

be a commutative diagram of R-modules and R-module homomorphisms with exact rows. Prove that

    (a) if f', α, and γ are injective, then β is injective.

    (b) if β is surjective, γ and f' are injective, then α is surjective.

6. (10 pts) Prove or disprove the following statement:

    "If the field F is a finite dimensional extension of $\mathbb{Q}$, then F contains only a finite number of roots of unity."

7. (16 pts) Let $f(x) = x^5 - 14x + 7$ be a polynomial in $\mathbb{Q}[x]$. Suppose that $E \subseteq \mathbb{C}$ is the splitting field of $f(x)$ over $\mathbb{Q}$.

   (a) Show that $f(x)$ is irreducible over $\mathbb{Q}$.
   (b) Determine the Galois group $\mathrm{Aut}_{\mathbb{Q}}(E)$.

Modern Algebra Qualifying Exam

Fall 2025

1. Let $H \leq K$ be subgroups of a group G.

    (a) (10 %) Suppose K is cyclic and normal in G. Prove that H is also normal in G.

    (b) (8 %) Give an example where H is normal in K and K is normal in G, but H is not normal in G. Please explain your answer.

2. (a) (8 %) Prove that every group of order 45 is abelian.

    (b) (8 %) Is it true that every group of order 45 is cyclic? Please explain your answer.

3. Consider the ring $\mathbb{Z}[x]$ and the ideals

$$I = (x) = \big\{ x\, f(x) \mid f(x) \in \mathbb{Z}[x] \big\}, \text{ and}$$
$$J = (5, x^2 + 1) = \big\{ 5\, f(x) + (x^2 + 1)\, g(x) \mid f(x), g(x) \in \mathbb{Z}[x] \big\}.$$

    (a) (8 %) Prove that I is a prime ideal but not a maximal ideal.

    (b) (8 %) Find a maximal ideal M containing I. Please explain your answer.

    (c) (8 %) Prove that J is not a prime ideal.

4. (10 %) Let R be a ring and suppose $f : A \to B$ and $g : B \to A$ are homomorphisms of R-modules such that $gf = 1_A$. Prove that $B = \operatorname{Im} f + \operatorname{Ker} g$ and $\operatorname{Im} f \cap \operatorname{Ker} g = \{0\}$.

5. (a) (8 %) For the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}i)$, are they isomorphic as $\mathbb{Q}$-vector spaces? Please explain your answer.

    (b) (8 %) For the fields $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(\sqrt[4]{2}i)$, are they isomorphic as fields? Please explain your answer.

6. (a) (8 %) Please construct a field of 125 elements. Please explain your answer.

    (b) (8 %) If L is an algebraic closure of a finite field F, is it true that L is also a finite field? Please explain your answer.