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

1. Let G be a group and N, H be subgroups of G. Suppose that $N \lhd G$, $|H|$ 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 $\mathrm{Aut}_{\mathbb{Q}}F$. (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 $\operatorname{Ker} f$ 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 $M = \operatorname{Ker} f \oplus \operatorname{Im} f$. (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

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

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) ∈ 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

   $0 \to (M_2 \cap N)/(M_1 \cap N) \to M_2/M_1 \to (M_2 + N)/(M_1 + N) \to 0$. (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 $B = \mathrm{Im} f \oplus \mathrm{Ker}\, g$. (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 $G = \mathrm{Aut}_K(E)$ be the Galois group of f. Let $\Lambda = \{\, \alpha \in E \mid f(\alpha) = 0 \,\}$. We use $\mathrm{Sym}(\Lambda)$ 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 $\mathrm{Sym}(\Lambda)$. (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 $\mathrm{Aut}_{\mathbb{Q}}E$ 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

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

   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

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

   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 $\mathrm{Aut}_{\mathbb{Q}}(K)$ of $f(x)$.