Algebra **Ph.D. Entrance Exam** **Fall 2009**

September 3, 2009

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let H, K, N be subgroups of a group G such that H is a subgroup of K. Show that the following are equivalent.
   (a) $H = K$.
   (b) $H \cap N = K \cap N$ and $HN = KN$.

(2) Let G be a semigroup for which the cancellation laws are satisfied.
   (a) Prove that if G is finite, then G is a group.
   (b) Give an example of an infinite semigroup G for which the cancellation laws are satisfied that is not a group.

(3) Let G be a finite group and let P be a Sylow p-subgroup of G. Show that the following conditions are equivalent:
   (a) P is the only Sylow p-subgroup of G;
   (b) P is normal in G.

(4) Let G be a group, let $a \in G$ have order k, and let p be a prime divisor of k. Prove that if $x \in G$ and $x^p = a$, then x has order pk.

(5) Let H be a subgroup of the symmetric group S_n. Prove that the alternating group A_{n+2} has a subgroup isomorphic to H.

(6) Let R be a commutative ring with identity and prime characteristic p and let n be a positive integer. Show that the map $R \to R$ given by $r \mapsto r^{p^n}$ is a homomorphism of rings.

(7) Consider $R = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ as a subring of the reals. R can be considered either as a $\mathbb{Z}$-module or as an R-module. The map $f : R \to R$ is given by $f(a + b\sqrt{2}) = a + b$. Prove or disprove each of the following:
   (a) f is a $\mathbb{Z}$-homomorphism.
   (b) f is an R-homomorphism.

(8) Let $\mathbb{Z}[x]$ be the ring of polynomials with integral coefficients. Show that the ideal $I = (2, x)$ of $\mathbb{Z}[x]$ generated by the set $\{2, x\}$ is not principal.

(9) Let R be a ring, A, B be R-modules, and $f : A \to B$ and $g : B \to A$ be R-module homomorphisms such that $g \circ f$ is the identity map on A. Prove that B is isomorphic to the direct sum of $\operatorname{Im} f$ and $\ker g$.

(10) Let R be a commutative ring and I be an ideal in R. Prove that I is a free R-module if and only if I is a principal ideal in R generated by an element $a \in R$ that is not a zero divisor.

(11) Prove that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(12) Let F be an extension field of a field K, and let $u \in F$ be algebraic over K of degree relatively prime to 6. Prove that $K(u) = K(u^3)$.

(13) Let F be an algebraic extension field of a field K and let R be a subring of F such that $K \subseteq R$. Prove that R is a field. Show by giving a counterexample that it necessary to assume that the extension F/K is algebraic.

(14) Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^3 + 5x + 5$. Find $a, b, c \in \mathbb{Q}$ so that

$$\alpha^{-1} = a\alpha^2 + b\alpha + c.$$

(15) Prove that every algebraically closed field is infinite.

Ph.D. Entrance Examination in Algebra

April 2011

Instructions: Throughout this exam, $\mathbf{C}, \mathbf{Q}, \mathbf{Z}, \mathbf{Z}_m$ represent the complex number field, the rational number field, the ring of integers, and the cyclic group of order m, respectively. Work any ten problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded. (Otherwise only the first 10 problems will be counted.)

Notation and Definitions: For any subset X of a group G, $\langle X \rangle$ is the intersection of all subgroups of G that contain X. Thus $\langle X \rangle$ is the smallest subgroup of G containing X.

1. Let H be a normal subgroup of a group G and let $\pi : G \mapsto G/H$ given by $\pi(x) = xH$ be the canonical homomorphism. If $X \subseteq G$ is a subset such that $\langle \pi(X) \rangle = G/H$, show that $\langle H \cup X \rangle = G$.

2. Let S_n denote the symmetric group on n letters. Show that S_n can be generated by the two permutations $\sigma = (1\ 2)$ and $\tau = (1\ 2\ ...\ n-1\ n)$.

3. Let H and K be subgroups of G. If $|H|$ and $|K|$ are relatively prime, then $|H \cap K| = 1$.

4. Let G be a group of order $|G| = pq$, where p and q are primes such that $p > q$ and such that $q \not| (p-1)$. Show that G is abelian.

5. Is there a simple group of order 48? Present an example for a YES answer and a proof for a NO answer.

6. Let G be a finite group such that a prime p divides $|G|$. Prove or disprove the following statement: If H is a subgroup of G, then G has a Sylow p-subgroup S_p such that $S_p \cap H$ is a Sylow p-subgroup of H.

7. Let R, R' be two commutative rings with unity (multiplicative identity), and let $f : R \mapsto R'$ be a ring homomorphism. Let $I' \subseteq R'$ be an ideal of R'. Determine if each of the following is a correct statement. Give your proofs for a YES answer and counterexamples for a NO answer.
(i) If I' is a prime ideal in R', then $f^{-1}(I')$ is a prime ideal in R.
(ii) If I' is a maximal ideal in R', then $f^{-1}(I')$ is a maximal ideal in R.

8. Let $F = \mathbf{Z}_7$ denote the field of 7 elements. Answer each of the following questions: (You must prove or justify your answer.)

Ph.D. Entrance Examination in Algebra

April 2012

Directions: Work any 10 problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded. Without such indications, only the first 10 will be graded.

Notation: The symbols $\mathbf{Z}, \mathbf{Q}$ and $\mathbf{C}$ represents the rings of integers, rational numbers, and complex numbers, respectively. For a group G and its subgroup H, $[G : H]$ denotes the index of H in G. For fields $F \leq K$, (F, K are fields and $F \subseteq K$), $[K : F]$ represents the dimension of the F-vector space K.

1. Let G, H be groups and let $a \in G$ be an element of order 23. If $f : G \mapsto H$ is a group homomorphism such that $f(a)$ has order at least 2. Determine the order of $f(a)$.

2. Let H be a normal subgroup of a group G with a finite index $m = [G : H]$. Show that $\forall g \in G$, $g^m \in H$.

3. Let p be a prime and G be a finite group such that p divides $|G|$. Let P be a Sylow p-subgroup of G and N be a normal subgroup of G. If P is not a normal subgroup of G, show that PN/N is a Sylow p-subgroup of G/N.

4. If $p > q$ are primes, show that a group of order pq has at most one subgroup of order p.

5. Show that there is no simple group of order 56.

6. Let G be a finite group of order $n > 2$ and let p be a prime with $p|n$. If H be a p-subgroup of G, show that H is contained in a Sylow-p-subgroup S of G if and only if P is contained in the normalizer of S in G.

7. Let R be a commutative ring and let I be an ideal of R. Let M be an R-module. Show that

$$N = \{m \in M | sm = 0, \forall s \in I\}$$

is a submodule.

8. Let $R = \mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \ : \ a, b \in \mathbf{Z} \text{ and } (\sqrt{-5})^2 = -5\}$. (It is known that this is a subdomain of the complex number field).
(i) Show that every non zero element of R has a factorization into irreducibles in R.
(ii) Is R a UFD? Give a proof for a YES answer and give an example for a NO answer.

Ph.D. Entrance Examination in Algebra

April 2014

Directions: Work any 10 problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded. Without such indications, only the first 10 will be graded.

Notation: The symbols $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{C}$ represent the rings of integers, rational numbers, and complex numbers, respectively. For a group G and its subgroup H, $[G : H]$ denotes the index of H in G. The center of a group G is $Z(G) = \{g \in G \ : \ \forall x \in G, gx = xg\}$. For fields $F \leq K$, (F, K are fields and $F \subseteq K$), $[K : F]$ represents the dimension of K over F.

1. Let G be an abelian group and let $H = \{g \in G \ : \ g \text{ has finite order}\}$.
(i) Show that H is a subgroup of G.
(ii) Give an example to show that the statement might be false if G is not abelian.

2. Let G be a group and let $a \in G$. Show that if for some integers $p > 0$ and $q > 0$ with $\gcd(p, q) = 1$, the order of a is pq, then there exist elements $b, c \in G$ such that the order of b is p and the order of c is q.

3. Let G be a group with $|G| = 49$. Show that the center of G has at least 6 elements, and further show that G is abelian.

4. If $p > q$ are primes, show that a group G of order pq has exactly one subgroup of order p. Is G a simple group? (Justify your answer).

5. Let G be a group of order 85. Show that there is a homomorphism $f : G \to \mathbb{Z}_{17}$ such that $f(G) = \mathbb{Z}_{17}$.

6. Let R be a ring with more than one element which may or may not have a multiplicative identity. Suppose that for each $a \in R^* = R - \{0\}$, there is a unique $b \in R$ such that $aba = a$. Show that R has a multiplicative identity and is a division ring. (Hint: First show that R has no zero divisor and for a fixed $a \in R^*$, ab behaves like the multiplicative identity).

7. If $f : A \mapsto A$ is an R-module homomorphism such that $f \circ f = f$, then

$$A = \text{ Ker } f \oplus \text{ Im } f.$$

8. Let $R = \{a + b\sqrt{10} : a, b \in \mathbf{Z}\}$ be a subring of the field of $\mathbb{R}$.
(a) Show that the mapping $N : R \mapsto \mathbf{Z}$ given by $N(a + b\sqrt{10}) = a^2 - 10b^2$ is multiplicative (that is, $\forall u, v \in R$, $N(uv) = N(u)N(v)$) and $N(u) = 0$ if and only if $u = 0$.

(b) Show that $4 + \sqrt{10}$ is irreducible but not a prime in R.
(c) Is R an integral domain? a PID (principal ideal domain)? Justify your answer.

9. Let R be a commutative ring, and let M and N be two R-modules. Let $f : M \mapsto N$ be an R-module homomorphism. Show that $K = \{x \in M \ : \ f(x) = 0\}$ is a submodule of M and $W = \{f(x) \in N \ : \ x \in M\}$ is a submodule of N.

10. Let R be an integral domain and let P be an ideal of R such that R/P is also an integral domain with at least two elements. Show that for any $x, y \in R - P$, $xy \in R - P$.

11. Let $f(x) = x^{11} + 7x^9 - 14x^3 + 35 \in \mathbb{Z}[x]$ and F be a subfield of $\mathbb{C}$ such that $\mathbb{Q} \leq F$. If $[F : Q] = 120$, show that F does not contain any root of $f(x)$.

12. Let F be a field of order 81. Show that the equation $x^{20} = 1$ has at least two solutions in F.

13. Let $F < E$ be fields, and let $\alpha, \beta \in E - F$ such that α is a transcendental element over F. If $[F(\alpha, \beta) : F(\beta)] = 67$, is β an algebraic element over F? Justify your answer.

14. Let $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}$. Show that $\mathbb{Z}[\sqrt{-1}]/(7)$ is a field. (Hint: Show that the element 7 is irreducible in $\mathbb{Z}[\sqrt{-1}]$.)

15. Find the Galois group of $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ over $\mathbb{Q}$.

9. Let R be an integral domain and let P be an ideal of R such that R/P is also an integral domain. Show that for any $x, y \in R \setminus P$, $xy \in R \setminus P$. (That is, the multiplication of R, when restricted to the subset $R \setminus P$, is a binary operation.)

10. Let α be a root of $x^{11} - 5x^6 + 10$ in $\mathbf{C}$, and let β be a root of $x^{26} + 3x^6 - 6$ in $\mathbf{C}$. Show that $\alpha \notin \mathbf{Q}(\beta)$.

11. Let R be a division ring and let $M_n(R)$ denote ring all $n \times n$ matrices over R.
(i) Determine all matrices in $M_2(R)$ such that for any $B \in M_2(R)$, $AB = BA$.
(ii) Can you extend your conclusions to $M_n(R)$ for arbitrary integer $n > 0$? If so, state the generalization of (i) and outline a proof (no need for detailed proofs here.)

12. Let $F \leq K$ be fields such that K is a finite dimensional extension of F. Suppose that the Galois group $Aut_F K \cong S_3$, the permutation group of degree 3.
(i) If K is a Galois extension of F, how many fields E are there such that $F \leq E \leq K$? Justify your answer.
(ii) If we do not assume that K is a Galois extension of F, what can you say about the number of intermediate fields E such that $F \leq E \leq K$? Give an explanation for your answer.

13. Let F be a field of characteristic zero, and let D be the formal differentiation map. That is:

$$D(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) = a_1 + 2a_2x + ... + na_nx^{n-1}.$$

(i) Show that $D : F[x] \mapsto F[x]$ is a group homomorphism of $(F[x], +)$ onto itself. Is D a ring homomorphism?
(ii) Determine the kernel and the image of D.

14. Let F and K be fields such that K is a finite dimension extension of F. Prove or disprove the following statement: for any $\alpha \in K \setminus F$, there always exists a polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$ and the degree of $f(x)$ is a factor of $[K : F]$.

15. Let $p > 2$ be a prime and let $\mathbf{Z}_p$ denote the finite field of p elements. Show that if $f(x)$ is an irreducible polynomial in $\mathbf{Z}_p[x]$, then there exists an integer n such that $f(x)$ divides $x^{p^n} - x$ in $\mathbf{Z}_p[x]$.

(i) Is $F[x]/(x^2+x+6)$ a field?
(ii) Are the two quotient rings $F[x]/(x^2+3x+3)$ and $F[x]/(x^2+x+6)$ isomorphic?

9. Let R be a principal ideal domain. Let $a_1, a_2, \cdots, a_n \in R$. If the ideal (d) equals the ideal $(a_1, a_2, \cdots, a_n)$, show that d is a greatest common divisor of $a_1, a_2, \cdots, a_n$.

10. Let F be a field and $f(x) \in F[x]$ be a non-zero polynomial. Show that the following are equivalent:
(i) The ideal $(f(x))$ is a prime ideal in $F[x]$.
(ii) The ideal $(f(x))$ is a maximal ideal in $F[x]$.
(iii) The polynomial $f(x)$ is irreducible.

11. Let $f(x) = x^4 - 2$ be a polynomial over the rational number field. Show that $f(x)$ is irreducible and determine the order of the Galois group of $f(x)$. (That is, we want to know the number of elements in the Galois group of $f(x)$).

12. Let F be a finite field with multiplicative identity 1_F. and $\mathbf{Z}$ be the ring of integers. Define a ring homomorphism $f : \mathbf{Z} \mapsto F$ given by $f(1) = 1_F$. Show that there exists a prime integer $p > 0$ such that the kernel of f is (p).

13. Let R be a PID, and let $a_1, a_2, ..., a_n, ...$ be an infinite sequence of elements in R such that for each $n \geq 1$, $a_{n+1}|a_n$ (that is, $a_n = a_{n+1}r_n$ for some $r_n \in R$). Show that there exists an $N > 0$ such that for every $m \geq N$, R has a unit u_m satisfying $a_m = a_N u_m$.

14. Let $F \leq K$ be fields. Prove that if $[K : F]$ is finite, then for every $u \in K$, u is algebraic over F.

15. Let $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbf{Z}\}$ be a subset of $\mathbf{C}$. Do each of the following.
(i) Show that $\mathbf{Z}[\sqrt{-5}]$ an integral domain.
(ii) Is $\mathbf{Z}[\sqrt{-5}]$ a principal ideal domain?
(iii) Is $\mathbf{Z}[\sqrt{-5}]$ an unique factorization domain?
(You need to give a proof for YES answers and to present an example for NO answers to (ii) and (iii).)

Solutions:

Throughout this exam, $\mathbf{R}, \mathbf{Q}, \mathbf{Z}, \mathbf{Z}_m$ represent the real number field, the rational number field, the ring of integers, and the cyclic group of order m, respectively. Work any ten problems. If you turn in partial solutions to more than 10 problems, indicate clearly which 10 should be graded. (Otherwise only the worst 10 problems will be counted.)

1. Let H be a normal subgroup of a group G and let $\pi : G \mapsto G/H$ given by $\pi(x) = xH$ be the canonical homomorphism. If $X \subseteq G$ is a subset such that $\langle \pi(X) \rangle = G/H$, show that $\langle H \cup X \rangle = G$.

Proof: For any $g \in G, \pi(g) = gH \in G/H$. As $\langle \pi(X) \rangle = G/H$, there exist $x_1, x_2, ..., x_k \in X$ such that for some $r_i \in \{1, -1\}$, $gH = \prod_{i=1}^{k} (x_i H)_i^r = \prod_{i=1}^{k} x_i^{r_i} H$. It follows that there must be $h_1, h_2 \in H$ such that

$$gh_1 = \prod_{i=1}^{k} x_i^{r_i} h_2, \text{ and so } g = \prod_{i=1}^{k} x_i^{r_i} h_2 h_1^{-1}.$$

This implies $g \in \langle H \cup X \rangle$, and so $G \subseteq \langle H \cup X \rangle$.

2. Let S_n denote the symmetric group on n letters. Show that S_n can be generated by the two permutations $\sigma = (1\ 2)$ and $\tau = (1\ 2\ ...\ n-1,\ n)$.

Proof: Since any cycle $(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(1\ i_{k-1}) \cdots (i_1\ i_2)$. It suffices to show that σ and τ can generate all transpositions.

Note that $\tau\sigma\tau^{-1} = (2\ 3)$, $\tau(2\ 3)\tau^{-1} = (3\ 4)$, ... and so σ and τ can generate all transpositions of the form $(i,\ i+1)$. Since $(i\ i+1)(i+1\ i+2)(i,\ i+1) = (i\ i+2)$, all transpositions of the form $(i\ j)$ can be generated by σ and τ.

3. 3. Let H and K be subgroups of G. If $|H|$ and $|K|$ are relatively prime, then $|H \cap K| = 1$.

Proof: Since $|H \cap K|$ divides $|H|$ and $|H \cap K|$ divides $|K|$, $|H \cap K|$ is a common factor of $|H|$ and $|K|$.

4. Let G be a group of order $|G| = pq$, where p and q are primes such that $p > q$ and such that $q \not| (p-1)$. Show that G is abelian.

Proof: Let n_p, n_q denote the number of Sylow-p-subgroups and Sylow-q-subgroups of G, respectively. Then by the 3rd Sylow Theorem, $n_p | (pq)$ and $n_p \equiv 1 \pmod{p}$. Since $n_p | (pq)$, we have $n_p \in \{1, p, q\}$. Since $q < p$, $n_p = q$ violates $n_p \equiv 1 \pmod{p}$, and so $n_p = 1$. Thus G has only one subgroup H of order p, and so H is normal in G.

Similarly, $n_q | (pq)$ and $n_q \equiv 1 \pmod{q}$. Since $q \not| (p-1)$, $n_q = p$ is impossible. Thus $n_q = 1$, and so G has a normal subgroup K of order q.

Since p, q are primes, $H = (a)$ and $K = (b)$ are cyclic subgroups of G. Since p and q are distinct elements, $|H \cap K| = 1$. It follows that $|G| \geq |HK| = |H| \cdot |K|/|H \cap K| = |G|$. Since HK is a subgroup of G, $G = HK = \{a^i b^j \ : \ i, j \in \mathbf{Z}\}$, and so $G \cong H \times K \cong \mathbf{Z}_p \times \mathbf{Z}_q \cong \mathbf{Z}_{pq}$.

5. Is there a simple group with order 48? (Give your example for the YES answer, and present your proof for the NO answer).

Proof: Note that $48 = 2^4 \cdot 3$. Let n_2 denote the number of Sylow-2-subgroups of G. Then $n_2 \in \{1, 3\}$. If $n_2 = 1$, then G has a normal subgroup of order 16, and so it is not simple. Hence we may assume that $n_2 = 3$. Let H_1, H_2, H_3 be the Sylow-2-subgroups of G, and let $H = H_1 \cap H_2$. Then $48 \geq |H_1 H_2| = |H_1| \cdot |H_2|/|H| = 16^2/|H|$, and so by the fact that $|H|$ is a factor of 16, we have $|H| \geq 8$. Since $H_1 \neq H_2$, we have $|H| = 8$.

Now $[H_1 : H] = 2$ and $[H_2 : H] = 2$, and so H is a normal subgroup of both H_1 and H_2. It follows that if $N = N_G(H)$ is the normalizer of H in G, then both $H_1 \cup H_2 \subseteq N$. Thus $H_1 H_2 \subseteq N$, and so $|N| \geq |H_1 H_2| = 16^2/8 = 32$. But $|N|$ is also a factor of 48. This forces that $|N| = 48$ and so H is a normal subgroup of G.

Conclusion: either G has a normal subgroup of order 16 (Sylow 2-subgroup), or a normal subgroup of order 8. Therefore, G cannot be a simple group.

6. Let G be a finite group such that a prime p divides $|G|$. Prove or disprove the following statement: If H is a subgroup of G, then G has a Sylow p-subgroup S_p such that $S_p \cap H$ is a Sylow p-subgroup of H.

Proof: If p does not divide $|H|$, then for any Sylow p-subgroup S_p of G, $S_p \cap H$ consists of the identity and so is a Sylow p-subgroup of H.

Assume that p divides $|H|$. Let S' be a Sylow-p-subgroup of H. Then S' is a p-subgroup of G. By Sylow's first Theorem, there must be a Sylow p-subgroup S_p of G such that $S' \subseteq S_p$. Since S' is a maximal p-subgroup of H, $H \cap S_p = S'$.

7. Let R, R' be two commutative rings with unity (multiplicative identity), and let $f : R \mapsto R'$ be a ring homomorphism. Let $I' \subseteq R'$ be an ideal of R'. Determine if each of the following is a correct statement. Give your proofs for a YES answer and counterexamples for a NO answer.

(i) If I' is a prime ideal in R', then $f^{-1}(I')$ is a prime ideal in R.

(ii) If I' is a maximal ideal in R', then $f^{-1}(I')$ is a maximal ideal in R.

Proof: (i) Let $I = f^{-1}(I')$. We skip the routine to verify that I is an idea of R, and only present the proof that I is prime. Suppose that $ab \in I$. Then $f(a)f(b) = f(ab) \in I'$. Since I' is prime, either $f(a) \in I'$, whence $a \in I$; or $f(b) \in I'$, whence $b \in I$. This proves that I is prime.

(ii) does not always hold. Let R' be a field, and let $I' = \{0\}$. Then I' is maximal.

8. Let $F = \mathbf{Z}_7$ denote the field of 7 elements. Answer each of the following questions: (You must prove or justify your answer.)
(i) Is $F[x]/(x^2 + x + 6)$ a field?
(ii) Are the two quotient rings $F[x]/(x^2 + 3x + 3)$ and $F[x]/(x^2 + x + 6)$ isomorphic?

Proof: Let $g(x) = x^2 + x + 6$. Computing $g(0) = 6, g(1) = 1$, $g(2) = 5, g(3) = 4$, $g(4) = 5, g(5) = 1$ and $g(6) = 6$ in Z_7. Since the degree of G is 2, g is irreducible, and so $F[x]/(x^2 + x + 6)$ is a field.
(ii) Let $f(x) = x^2 + 3x + 3$. Then $f(1) = 0$ in Z_7, and so $f(x)$ is reducible. This implies that $F[x]/(x^2 + 3x + 3)$ is not a field, and so they cannot be isomorphic.

9. Let R be a principal ideal domain. Let $a_1, a_2, \cdots, a_n \in R$. If the ideal (d) equals the ideal $(a_1, a_2, \cdots, a_n)$, show that d is a greatest common divisor of $a_1, a_2, \cdots, a_n$.

Proof: Since $(d) = (a_1, a_2, \cdots, a_n)$, each $a_i = dr_i$ for some $r_i \in R$. Hence d is a common divisor of $a_1, a_2, \cdots, a_n$. If d' is also a common divisor of $a_1, a_2, \cdots, a_n$, then as $d \in (a_1, a_2, \cdots, a_n)$, $d'|d$, and so d is a greatest common divisor of $a_1, a_2, \cdots, a_n$.

10. Let F be a field and $f(x) \in F[x]$ be a non-zero polynomial. Show that the following are equivalent:
(i) The ideal $(f(x))$ is a prime ideal in $F[x]$.
(ii) The ideal $(f(x))$ is a maximal ideal in $F[x]$.
(iii) The polynomial $f(x)$ is irreducible.

Proof:

10. Let $f(x) = x^4 - 2$ be a polynomial over the rational number field. Show that $f(x)$ is irreducible and determine the order of the Galois group of $f(x)$. (That is, we want to know the number of elements in the Galois group of $f(x)$).

Proof:

12. 12. Let F be a finite field with multiplicative identity 1_F. and $\mathbf{Z}$ be the ring of integers. Define a ring homomorphism $f : \mathbf{Z} \mapsto F$ given by $f(1) = 1_F$. Show that there exists a prime integer $p > 0$ such that the kernel of f is (p).

Proof:

13. Let R be a PID, and let $a_1, a_2, ..., a_n, ...$ be an infinite sequence of elements in R such that for each $n \geq 1$, $a_{n+1}|a_n$ (that is, $a_n = a_{n+1}r_n$ for some $r_n \in R$). Show that there exists an $N > 0$ such that for every $m \geq N$, R has a unit u_m satisfying $a_m = a_N u_m$.

Proof: By assumption, $(a_n) \subseteq (a_{n+1})$ for all n. Use the definition of ideals to verify that $\cup_{n\geq 1}(a_n)$ is also an ideal. Since R is a PID, there must be an $a \in R$, such that

$(a) = \cup_{n\geq 1}(a_n)$. As $a \in (a)$, there must be an N such that $a \in (a_N)$. On the other hand, as $a_N \in (a_N) \subseteq (a)$, we must have $(a) = (a_N)$. For any $m \geq N$, $a_m \in (a) = (a_N)$. Thus for some $r_m \in R$, $a_m = u_m a_N$. But $a_N \subseteq (a_m)$ and so for some $r_N \in R$, $a_N = a_m r_R$. Hence $a_m = u_m a_N = u_m r_N a_m$. It follows by the assumption that R is an integral domain that $u_m r_N = 1$, and so u_m is a unit of R.

14. Let $F \leq K$ be fields. Prove that if $[K : F]$ is finite, then for every $u \in K$, u is algebraic over F.

Solution: Let $n = [K : F]$. Then $1, u, u^2, \cdots, u^n$ are $n+1$ vectors in the vector space K over F, and so there must be scalars $a_0, a_1, \cdots, a_n$, not all zero, such that $a_0 + a_1 u + a_n u^n = 0$. This implies that u must be algebraic.

15. Let $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbf{Z}\}$ be a subset of $\mathbf{C}$. Do each of the following.
(i) Show that $\mathbf{Z}[\sqrt{-5}]$ an integral domain.
(ii) Is $\mathbf{Z}[\sqrt{-5}]$ a PID?
(iii) Is $\mathbf{Z}[\sqrt{-5}]$ a UFD?
(You need to give a proof for YES answers and to present an example for NO answers to (ii) and (iii).)

Sketch of Proof: (i) Note that $\mathbf{C}$ is a field. To show that $\mathbf{Z}[\sqrt{-5}]$ is a domain, it suffices to show that $1 \in \mathbf{Z}[\sqrt{-5}]$, and $\mathbf{Z}[\sqrt{-5}]$ is closed under addition and multiplication.
(iii) and (ii) As $21 = (3)(7) = (1 + 2(\sqrt{-5})(1 - 2\sqrt{-5})$, it is not a USF, and so it cannot be a PID. How do we get 21? Note that $(a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$, we need to find a composite number with the form of $a^2 + 5b^2$. Thus $6 = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$ can be found as another example.

Algebra **Ph.D. Entrance Exam** **Fall 2010**

September 1, 2010

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let m and n be positive integers. Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a cyclic group if and only if m, n are relatively prime.

(2) Let G be a group and H be the group of inner automorphisms of G under composition, that is, let H consist of all automorphisms $\varphi_a : G \to G$ with $a \in G$ given by $\varphi_a(g) = aga^{-1}$. Prove that H is isomorphic to G/Z, where $Z = Z(G)$ is the center of G.

(3) Let G be a group, H be a subgroup of G, and S be the set of left cosets of H in G. Let G act on S by multiplication, that is, the action is defined by $g(aH) = (ga)H$ for any $a, g \in G$. Show that the kernel of the action is $\bigcap_{g \in G} gHg^{-1}$.

(4) Let G be a finite group, p be a prime, P be a Sylow p-subgroup of G and N be a normal subgroup of G. Prove that PN/N is a Sylow p-subgroup of G/N.

(5) Show that there are no simple group of order 30.

(6) Let R be a commutative ring with 1 that has exactly two ideals. Prove that R is a field.

(7) Let R, S be commutative rings, P be a prime ideal in S, and $f : R \to S$ be a ring homomorphism. Prove that the preimage $f^{-1}(P)$ is a prime ideal in R.

(8) Show that the polynomial ring $\mathbb{Z}[x]$ is not a principal ideal domain.

(9) Give an example of a ring R and two functions $f, g : R \to R$ such that
   (a) f is a ring homomorphism but not an R-homomorphism (homomorphism of R-modules);
   (b) g is an R-homomorphism but not a ring homomorphism.

(10) Let R be a commutative ring with 1 and M be a cyclic R-module. Prove that there is an ideal I of R such that M is isomorphic to the R-module R/I.

(11) Let α be a root of $x^7 + 5x^4 - 25x + 15$ in $\mathbb{C}$ and F be a subfield of $\mathbb{C}$ with $[F : \mathbb{Q}] = 36$. Prove that $\alpha \notin F$.

(12) Let F be a field and K be an algebraic extension of K such that every polynomial in $F[x]$ splits over K. Prove that K is algebraically closed.

(13) Find the Galois group of the polynomial $\left(x^2 - 2\right)\left(x^2 - 3\right)$ over $\mathbb{Q}$.

(14) Let F, K be finite fields with F having m elements and K being an extension of F. Prove that there is a positive integer k such that K has m^k elements.

(15) Let K be a Galois extension of a field F with $n = [K : F] \in \mathbb{Z}$ and let $L_1, \ldots, L_m$ be intermediate fields where $m = 2^n$. Prove that $L_i = L_j$ for some $i \neq j$.

Algebra **Ph.D. Entrance Exam** **Fall 2011**

September 1, 2011

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

1. Let G be a finite group of order m. Let H, K be subgroups of G with $|H| = |K| = n$ and H being normal in G. Prove that if n and m/n are relatively prime, then $K = H$. Give a counterexample showing that without the assumpion of normality of H the statement is false.

2. Let $K \subseteq L$ be fields and $s \in L$ be such that $[K(s): K]$ is infinite. Prove that $[F(s): F]$ is also infinite for every subfield F of K.

3. Let M be a finitely generated R-module over a commutative ring R. Prove that there is a positive integer n and a submodule N of the R-module R^n such that M is isomorphic to the quotient module R^n/M.

4. Let K be a field extension of F generated by $a, b \in K$ of relatively prime degrees m and n over F. Prove that $[K: F] = m\,n$.

5. Let $\alpha, \beta \in \mathbb{C}$ be roots of some irreducible quadratic polynomials over $\mathbb{Q}$. Prove that if $F(\alpha)$ and $F(\beta)$ are not equal, then they are not isomorphic as rings. Are they isomorphic as additive groups?

6. Let D be an integral domain that is not a field and F be its field of fractions. Prove that F is not a free D-module.

7. Let K be a field extension of F and D be a ring such that $F \subseteq D \subseteq K$. Prove that if every element of D is algebraic over F, then D is a field. Give a counterexample showing that without the assumption of algebraicity, D does not have to be a field.

8. Find the degree of K over $\mathbb{Q}$, where K is the splitting field of $(x^2 + 1)(x^3 - 2)$. What is $\left[K\left(\sqrt{3}\right): K\right]$?

9. Let G be a finite group of order m acting nontrivially on a finite set S with n elements. (Nontrivially means that $ga \neq a$ for some $g \in G$ and $a \in S$.) Prove that if m does not divide $n!$, then G is not simple.

10. Can an infinite group have finitely many subgroups? Give a proof or a counterexample.

11. Prove that there are no simple groups of order 380.

12. Let G be a finite group whose order is 7^{23}. Prove that G has a nontrivial center.

13. Let R be a commutative ring and I be an ideal in R. Prove that I is maximal if and only if R/I is a field.

14. Prove that every Euclidean Domain is a Principal Ideal Domain.

15. Let D be a Principal Ideal Domain and I be a nonzero prime ideal in D. Prove that I is maximal.

Algebra **Ph.D. Entrance Exam** **Fall 2012**

August 30, 2012

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

1. Let G be a group, G' be the commutator subgroup of G, and N be a normal subgroup of G such that $N \cap G' = \{e\}$ (where e is the identity of G). Prove that $N \subseteq C(G)$, (where $C(G)$ is the center of G).
2. Give an example of a group G and two elements $a, b \in G$ of finite order such that the order of ab is infinite.
3. Let G be a group of order 96. Prove that G is not simple.
4. Let G be a subgroup of the symmetric group S_5. Prove that G is isomorphic to a subgroup of the alternating group A_7.
5. Prove that if $\sigma \in S_n$ is a product of two disjoint cycles and $\tau \in S_n$ is arbitrary, then $\tau^{-1}\sigma\tau$ is also a product of two disjoint cycles.
6. Let K be a field extension of a field F and $a_0, a_1, ...$ be a sequence of elements of K such that $[F(a_i) : F]$ is at most 6 each i. Let $b \in F(a_0, a_1, ...)$. Prove that $[F(b) : F]$ is not divisible by 7.
7. Let F be a field and $f(x) \in F[x]$ be a nonzero polynomial. Prove that if K is a field extension of F, $a \in K$ is a root of $f(x)$, and σ is an element of the Galois group of K over F, then $\sigma(a)$ is also a root of $f(x)$. Show also how that implies that if K is a splitting field of a polynomial of degree n over F, then the Galois group of K over F can have at most $n!$ elements.
8. Let F be a field, D be a ring that is not a field, and K be a field such that $F \subseteq D \subseteq K$. Prove that $[K : F]$ is infinite.
9. Let a be a root of the polynomial $x^3 - 6x + 3 \in \mathbb{Q}[x]$. Express the inverse a^{-1} as a linear combination of 1, a, and a^2 with rational coefficients.
10. Let R be a finite integral domain. Prove that R is a field.
11. Let F be a field and $R = F[x, y]$ be the ring of polynomials in variables x and y. Prove that R is not a Euclidean Domain.
12. Give an example of an integral domain D and a nonzero prime ideal in D that is not maximal.
13. State and prove the Eisenstein criterion for irreducibility in $\mathbb{Q}[x]$ of polynomials that belong to $\mathbb{Z}[x]$.
14. Prove that $\mathbb{Q}$ as a $\mathbb{Z}$-module is torsion-free but not free. (An R-module M is torsion-free if no nonzero element of M has a nonzero annihilator in R.) Is there a $\mathbb{Z}$-module that is free but not torsion-free. Give a proof or a counterexample.
15. Give an example of a ring R and functions $f, g : R \to R$ such that f is a ring homomorphism but not an R-module homomorphism, and g is an R-module homomorphism but not a ring homomorphism.

Algebra **Ph.D. Entrance Exam** **Fall 2013**

August 28, 2013

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let G be a finite group acting on a finite set S. Prove that the order of any orbit of the action is a divisor of the order of G.
(2) Let G be a group and H be the subgroup of G generated by a set $S \subseteq G$ such that $asa^{-1} \in S$ for any $s \in S$. Prove that H is a normal subgroup of G.
(3) Let m and n be positive integers. Prove that $\mathbb{Z}_m \times \mathbb{Z}_n$ is a cyclic group if and only if m, n are relatively prime.
(4) Let $p > 5$ be a prime. Prove that no group of order 12p can be simple.
(5) Let G be a group and H be the group of inner automorphisms of G under composition, that is, let H consist of all automorphisms $\varphi_a : G \to G$ with $a \in G$ given by $\varphi_a\left(g\right) = aga^{-1}$. Prove that H is isomorphic to G/Z, where $Z = Z(G)$ is the center of G.
(6) Let F be a field and f be a polynomial over F. Prove that there exists an extension K of F such that f has a root in K.
(7) Let K be a field extension of F and $f(x) \in F[x]$. Prove that if σ is an automorphism of K over F and $a \in K$ is a root of f, then $\sigma(a)$ is also a root of f.
(8) Let K be a field extension of F and $a \in K$ be algebraic over F. Prove that the field $F(a)$ is finitely dimensional over F.
(9) Prove that no finite field is algebraically closed.
(10) Write the multiplication table of a field with 8 elements.
(11) Let R be a commutative ring with identity of prime characteristic p and let n be a positive integer. Show that the map $f : R \to R$ given by $f(a) = a^{p^n}$ is a homomorphism of rings.
(12) Let $\mathbb{Z}[x]$ be the ring of polynomials with integral coefficients. Show that the ideal I of $\mathbb{Z}[x]$ generated by the set $\{2, x\}$ is not principal.
(13) Let D be a principal ideal domain and $\mathscr{C}$ be a set of nonzero ideals of D such that $\bigcap_{I \in \mathscr{C}} I = \{0\}$. Prove that $\mathscr{C}$ is infinite.
(14) Let D be a unique factorization domain and g, h be primitive polynomials over D. Prove that the product gh is also primitive.
(15) Let D be a principal ideal domain and $a, b \in D$ be relatively prime. Prove that there are $c, d \in D$ with $1_D = ac + bd$.

Algebra **Ph.D. Entrance Exam** **Fall 2014**

August 25, 2014

Directions: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded the first 10 problems will be graded. Start each solution on a clean sheet of paper.

(1) Let G be a group with subgroups K and H where H is an abelian normal subgroup of G and $K \subseteq H$.
   (a) Does it follow that K is normal in G? Give a proof or a counterexample.
   (b) What is the answer to the previous question if we assume that H is cyclic? Give a proof or a counterexample.

(2) Let S_n denote the group of permutations of the set $\{1, 2, \ldots, n\}$. Show that S_n can be generated by the two permutations: $(1\ 2)$ and $(1\ 2 \ldots n-1\ n)$.

(3) Let G be a finite group acting on a finite set S and $a \in S$. Prove that the size of the orbit containing a is equal to the index of some subgroup H of G. (Define this subgroup.)

(4) Let G be a group of order pq, where p and q are primes such that $p > q$ and such that q does not divide $p-1$. Show that G is isomorphic to the product $\mathbb{Z}_p \times \mathbb{Z}_q$ of cyclic groups of orders p and q, respectively.

(5) Let G be a finite group and H be a subgroup of G such that the index $p = [G : H]$ is the smallest prime dividing the order of G. Prove that G has a normal subgroup of index p.

(6) Let D be a principal ideal domain and $a, b \in D$ and d be a greatest common divisor of a and b. Prove that there are $s, t \in D$ such that $d = sa + tb$.

(7) Let R be a ring such that $x + x = 0$ and $xx = x$ for every $x \in R$. Prove that R is commutative.

(8) Let R be a commutative ring with identity and I be a proper ideal of R. Prove that there exists a maximal ideal of R that contains I.

(9) Let R be a ring with identity and M be a module over R that is generated by a finite subset A of M. Prove that M is isomorphic to a quotient module of R^A, which is the module over R consisting of all functions $f : A \to R$ with the standard operations.

(10) Give an example of a ring R and two functions $f, g : R \to R$ such that:
   (a) f is a ring homomorphism but is not an R-homomorphism (homomorphism of R-modules);
   (b) g is an R-homomorphism but not a ring homomorphism.

(11) Let K be a field extension of a field F and $a \in K$ be such that the degree $[F(a) : F]$ of $F(a)$ over F is finite. Prove that a is algebraic over F.

(12) Let K be a field extension of a field F and let L consists of all elements of K that are algebraic over F. Prove that L is a subfield of K.

(13) Let K be a finite Galois extension of a field F with the Galois group G and let E be an intermediate field that is normal over F. Prove that the Galois group of K over E is normal in G.

(14) Let g be an automorphism of the field $\mathbb{R}$ of real numbers such that $g(a) = a$ for every $a \in \mathbb{Q}$. Prove that g is the identity function.

(15) Let F be a field and f, g be polynomials over F. Prove that f and g have a non-constant factor in $F[x]$ if and only if there exists a field extension K of F and $a \in K$ that is a root of both f and g.

Ph. D. Entrance Exam—Algebra
April , 2016

Direction: Solve 10 of the following problems. Mark which of the problems are to be graded. Without clear indication which problems are to be graded, the first 10 problems will be graded.

Notes: For all problems in this exam, rings may or may not have multiplicative identities. You should NOT assume that a ring has an multiplicative identity unless it is clearly stated in the problem. And you should NOT assume that a ring homomorphism maps the identity to identity either.

1. Let G be a finite group with $|G| = n$ and let S be a subset of G with $|S| > \frac{n}{2}$. Prove that for each element $g \in G$, there exist elements $a, b \in S$ such that $g = ab$.

2. Let G be a finite group. Suppose that there is an automorphism $\alpha \in Aut(G)$ such that $\alpha(g) \neq g$ for any $g \neq e$ and $\alpha^2 = 1_G$.

   (1) Let $H = \{g^{-1}\alpha(g) | g \in G\}$. Show that $H = G$.

   (2) Show that $\alpha(a) = a^{-1}$ for all $a \in G$. (Hint: apply (1)).

   (3) Show that the order of G is odd and G is abelian.

3. Let M and N be two normal subgroups of G. If $M \cap N = \{e\}$, then for each $a \in M$ and each $b \in N$, $ab = ba$.

4. If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

5. If $|G| = pn$, with $p > n$, p prime, and H is a subgroup of order p, then H is normal in G.

6. Is there a simple group of order 48? Present an example for a YES answer and a proof for a NO answer.

7. Let $R = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}$ be a subring of the field of real numbers.

   (a) Show that the mapping $N : R \to \mathbb{Z}$ given by $N(a + b\sqrt{10}) = a^2 - 10b^2$ is multiplicative (that is, for any $u, v \in R$, $N(uv) = N(u)N(v)$) and $N(u) = 0$ if and only if $u = 0$.

   (b) Show that u is a unit in R if and only if $N(u) = \pm 1$.

   (c) Show that $4 + \sqrt{10}$ is an irreducible element o f R but not prime.

8. Let R be a ring such that for each $a \in R$, $a^2 = a$. Prove that R is commutative and $a + a = 0$.

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

   (a) $f^{-1}(J)$ is an ideal in R that contains Ker$f$.

   (b) If f is surjective, then $f(I)$ is an ideal in S.

10. Show that an integral domain with finitely many ideals is a field.

11. Let K/F be a field extension and $a \in K$ be algebraic over F. Prove that $a + 1$ is algebraic over F.

12. Let u be a root of the polynomial $x^3 - 3x - 1$ over $\mathbb{Q}$. Express both $u^4 + 2u^3 + 3 \in \mathbb{Q}$ and its inverse as linear combinations (over $\mathbb{Q}$) of $\{1, u, u^2\}$.

13. Let $E = \mathbb{Q}(\sqrt{5}, \sqrt{7})$. Show that E is a simple extension of $\mathbb{Q}$, and find a polynomial $f(x) \in \mathbb{Q}[x]$ such that $E \cong \mathbb{Q}[x]/(f(x))$.

14. Draw the lattice of all of the intermediate fields between $\mathbb{Q}$ and E where E is the splitting field of $x^4 - 2$ over $\mathbb{Q}$. Find $\mathrm{Gal}(E/F)$ for each of these intermediate fields F.

15. Show that $F_{p^n} \subseteq F_{p^m}$ if and only if n divides m.

Ph.D. Entrance Exam in Algebra
April 17, 2017

Instructions – Please read carefully before you start.

- This exam has three parts:
  Part A: Group Theory, Part B: Field and Galois Theory, and Part C: Ring and Module Theory.

- **Work on a total of 7 questions**: ***work on two questions from each part, and one additional question from any part you want (Part A or Part B or Part C), for a total of 7 questions. Clearly indicate the questions from each part you worked on.***

- **In answering the questions, state and write any theorems you use carefully and separately**.

- You should not interpret any of the exam questions as trivial by referring to a result from a textbook or any lecture notes.

- Please **write big and legibly**. Justify your arguments with complete sentences using correct grammar. Solutions, even correct, without appropriate justifications or those that cannot be read, will not receive full credit.

- No electronic devices, calculators, cell phones, etc. are allowed during the exam.

- You have **3 hours** to complete the exam (4:00 PM - 7:00 PM).

Exam Questions

PART A: Group Theory

Conventions.
- $\mathrm{Z}(G)$ denotes the *center* of a given group G.
- $|A|$ denotes the *cardinality* of a set A.
- An action of a group G on a set S is said to be *transitive* if there is only one orbit of the action.

1. Prove that there is no group G such that $|G/\mathrm{Z}(G)| = 17$.

2. Let G be a finite group with $|G| = 4 \cdot 3^s$, where $s \geq 2$ is an integer. Prove that G is *not* simple.

3. Let G be a finite group and let S be a finite set with $|S| \geq 2$. Assume G acts *transitively* on S. Prove that there is an element $g \in G$ such that $g \cdot s \neq s$ for *all* $s \in S$.

4. Let G be a finite group with $|G| = 969$. Prove that G is *solvable*. (Note $969 = 3 \cdot 17 \cdot 19$)

5. Let G be a *finite* group, and let H and K be two subgroups of G. Assume P is a Sylow p-subgroup of H, and H is a subgroup of K. If P is a *normal* subgroup of H, and H is a *normal* subgroup of K, prove that P is a *normal* subgroup of K.

PART B: Field and Galois Theory

Conventions.
- A *Galois* extension is a field extension that is finite, normal and separable.
- $\mathbb{Q}$ denotes the set of rational numbers.

1. Prove that every algebraically closed field is infinite.

2. Prove that i and $\sqrt{2}$ belong to the splitting field K of the polynomial $p(x) = x^4 + 2$ over $\mathbb{Q}$.

3. Let $E = \mathbb{Q}\left(\sqrt[3]{2}\right)$. Prove that E is *not* a subfield of $\mathbb{Q}(w)$, where w is a *primitive* nth root of unity.

4. Let $F = \mathbb{Q}$, $\alpha = \sqrt{2 + \sqrt{2}}$, and $K = F(\alpha)$. Prove that K/F is a *Galois* extension with a *cyclic* Galois group of order 4.

5. Find, *using Galois Theory*, a primitive element for $\mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p and q are distinct prime integers.

PART C: Ring and Module Theory

Conventions.
• Assume all rings have multiplicative identity 1 such that $1 \neq 0$, and all modules considered are left modules.
• An element x of a ring R is said to have a *left inverse* if there exists $y \in R$ such that $yx = 1$.
• An element x of a ring R is said to be a *unit* if there exists $z \in R$ such that $xz = zx = 1$.
• A nonzero element a of a ring R is said to be a *zero-divisor* on R if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.

1. Let R be a ring (not necessarily commutative) and let $a, b \in R$. If $1 - ba$ has a left inverse in R, prove that $1 - ab$ has a left inverse in R.

2. Let R be a ring (not necessarily commutative) and let I be a nonzero left ideal of R. Assume the following conditions hold:

   (a) if J is a nonzero left ideal of R and $J \subseteq I$, then $J = I$.

   (b) if $0 \neq x \in I$, then x is *not* a zero-divisor on R.

   Prove that every nonzero element of R is a unit.

3. Let R be a commutative ring and let I and J be nonzero ideals of R. Assume $IJ = (b)$, that is, the product IJ of I and J is a *principal* ideal of R generated by some element $b \in R$. If b is *not* a zero-divisor on R, prove that I is a finitely generated ideal of R.

4. Let R be a ring (not necessarily commutative), M be an R-module, and let N be an R-submodule of M. Assume the following condition holds for the module N: whenever there is an ascending chain of R-submodules of N of the form

   $$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_n \subseteq N_{n+1} \subseteq \cdots$$

   there exists a positive integer k such that $N_k = N_{k+1} = N_{k+2} = \cdots$, that is, $N_k = N_{k+i}$ for all $i \geq 1$.

   If $f : N \to M$ is a surjective R-module homomorphism, prove that f is an isomorphism.

5. Let R be a ring (not necessarily commutative). An R-module P is said to be *projective* if it is a *direct summand* of a free R-module, that is, $F = P \oplus M$ for some free R-module F and some R-module M.

   If $e \in R$ is an *idempotent* element, that is, $e^2 = e$, prove that the R-module Re is projective.

   (Recall that Re is the cyclic R-module $\{re : r \in R\}$.)