

**CAPITAL NORMAL UNIVERSITY, 2026 SPRING**  
**ABSTRACT ALGEBRA II**

- (1) Find the number of isomorphism classes of groups of order 45.
- (2) For a given positive integer  $n$ , prove that there are at most  $\binom{n!-1}{n-1}$  isomorphism classes of groups of order  $n$ .
- (3) Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be two ideals of a commutative ring  $R$ . If an ideal  $I$  of  $R$  satisfies  $I \subseteq \mathfrak{p} \cup \mathfrak{q}$ , prove that  $I \subseteq \mathfrak{p}$  or  $I \subseteq \mathfrak{q}$ .
- (4) If a ring  $R$  has  $m$  non-zero left zero-divisors and  $m > 1$ , prove that  $\#R \leq (m+1)^2$ .
- (5) Let  $F[0, 1]$  be the set of all real-valued functions on the closed interval  $[0, 1]$ . Prove that  $F[0, 1]$  forms a commutative ring under point-wise addition and multiplication, and that  $I = \{f \in F[0, 1] : f(0) = 0\}$  is a maximal ideal of  $F$ .
- (6) Let  $n \geq 2$  be a positive integer. Prove that  $x^{n-1}y^2 + x^n + 2x^{n-1}y + x^{n-1} + xy + x + y + 1$  is an irreducible element in  $\mathbb{Q}[x, y]$ .
- (7) Let  $R$  be a ring, suppose  $M, N$  are left  $R$ -modules. If  $f : M \rightarrow N$  and  $g : N \rightarrow M$  are  $R$ -morphisms and  $g \circ f : M \rightarrow M$  is an automorphism, prove that  $N = \ker(g) \oplus \text{im}(f)$ .
- (8) Prove that  $\#\text{GL}_n(\mathbb{F}_p)$  is a factor of  $(p^n - 1)!$ .
- (9) Let  $R$  be a principal ideal domain. Prove that every prime ideal in  $R[x]$  can be generated by at most two elements.
- (10) If  $F/K$  is an algebraic extension and  $D$  is a subring such that  $K \subseteq D \subseteq F$ , prove that  $D$  is a field. Does this conclusion still hold if  $F/K$  is not algebraic?
- (11) Let  $R$  be a ring, and  $n_0 > 1$  be a positive integer. Assume that for any  $x \in R$ ,  $x^{n_0} = 0$  implies  $x = 0$ . Prove that if  $x_1, \dots, x_n \in R$  satisfy  $x_1x_2 \cdots x_n = 0$ , then  $x_{\sigma(1)}x_{\sigma(2)} \cdots x_{\sigma(n)} = 0$  for any permutation  $\sigma \in S_n$ .
- (12) Let  $u$  be an algebraic number over  $\mathbb{Q}$ , and let  $x^3 + 2x - 1$  be its minimal polynomial over  $\mathbb{Q}$ . Find the minimal polynomial of  $u^2 + u$  over  $\mathbb{Q}$ .
- (13) Let  $g(x)$  and  $h(x)$  be polynomials over a field  $K$ , and let  $u$  be a root of  $g(x)$  in a field extension  $L/K$ . Prove that  $g(h(x))$  is irreducible over  $K$  if and only if  $g(x)$  is irreducible over  $K$  and  $h(x) - u$  is irreducible over  $K(u)$ .
- (14) Let  $u$  be an algebraic element over  $K$ , prove that  $[K(u) : K] \leq n \cdot [K(u^n) : K]$ , where  $n > 0$  is an integer.
- (15) [Wilson] Let  $p$  be a prime number. Prove that  $(p-1)! \equiv -1 \pmod{p}$ .
- (16) Let  $E/F$  be a finite Galois extension, and let  $f \in F[x]$  be the minimal polynomial of  $u \in E \setminus F$  over  $F$ . Prove that for any two roots  $r_1, r_2$  of  $f$ , there exists  $\sigma \in \text{Gal}(E/F)$  such that  $\sigma(r_1) = r_2$ .
- (17) Let  $G$  be a finite abelian group. Prove that there exists a finite extension  $F/\mathbb{Q}$  such that  $\text{Gal}(F/\mathbb{Q}) \cong G$ . [Hint: if  $a$  and  $d$  are coprime positive integers, then there are infinitely many primes  $p$  such that  $p \equiv a \pmod{d}$ ]
- (18) Let  $E/F$  be a finite separable extension. Prove that  $E/F$  is Galois if and only if any irreducible polynomial in  $F[x]$  factors into a product of irreducible polynomials of the same degree in  $E[x]$ .
- (19) Let  $\mathbb{Q}(u)/\mathbb{Q}$  be a finite extension, and let  $L/\mathbb{Q}$  be the Galois closure of  $\mathbb{Q}(u)/\mathbb{Q}$ . If  $p$  divides  $[L : \mathbb{Q}]$ , prove that there exists a subfield  $F$  of  $L$  such that  $[L : F] = p$  and  $L = F(u)$ .
- (20) Let  $E/F$  be a finite Galois extension and let  $\text{Gal}(E/F)$  be a cyclic group. Prove that there is an isomorphism  $E^\times/F^\times \cong \ker(N_{E/F})$ , where  $N_{E/F} : E^\times \rightarrow F^\times$  is the norm map.
- (21) Let  $F \subseteq \text{Mat}_n(\mathbb{Q})$  be a field. Prove that  $[F : \mathbb{Q}I_n] \leq n$ , where  $\mathbb{Q}I_n := \{r \cdot I_n : r \in \mathbb{Q}\}$ .