Problems marked with (EC) are optional extra credit problems. These extra credit problems, however, are problems that a student interested in graduate school should try to do.

0.3: Functions

1. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = x + y$.
   (a) Determine, with proof, whether or not f is injective.
   (b) Determine, with proof, whether or not f is surjective.
2. Let $g : \mathbb{R} \to \mathbb{R}^2$ be defined by $g(x) = (x^2, e^x)$.
   (a) Describe the set $g^{-1}(0, 1)$ (by listing its elements with proper notation).
   (b) Describe the set $g^{-1}(1, 1)$.
   (c) Determine, with proof, whether or not g is injective.
   (d) Determine, with proof, whether or not g is surjective.
3. Given the functions f and g defined in the previous two problems, give the domains, codomains and rules for $f \circ g$ and $g \circ f$.

0.6: Common proof techniques

4. Write a useful denial of each statement (recall that a denial of statement P is any statement logically equivalent to "not P"):
   (a) For all $g \in G$, there is an $h \in G$ such that $gh = x$.
   (b) There exists a function $f : \mathbb{R} \to \mathbb{R}$ such that f is monstrous or f is tiny.
5. Write the contrapositive and converse of each statement:
   (a) If t is a turkey, then t gobbles and we eat t on Thanksgiving.
   (b) All animals are goats.
6. Prove that there is a prime number between 100 and 110.
7. Prove that there is no greatest element of the interval $(0, 1)$.

   Hint: Suppose that there is a greatest integer (say x), and produce a contradiction.
8. Prove that the sum of a rational number and an irrational number is irrational. (You may assume that the sum of two rational numbers is rational.)
9. Let $r \in \mathbb{R} - \{1\}$. Prove that for all $n \in \mathbb{N}$,

$$\sum_{j=0}^{n} r^j = \frac{r^{n+1} - 1}{r - 1}.$$

   Hint: Prove by induction on n.

1.1: Straightedge and compass constructions

10. Show that the intersection point(s) (x, y) of two distinct circles

$$(x - x_0)^2 + (y - y_0)^2 = r_0^2 \quad \text{and} \quad (x - x_1)^2 + (y - y_1)^2 = r_1^2$$

can be computed in terms of the constants x_0, y_0, r_0, x_1, y_1 and r_1 using (at worst) $+, -, \cdot, \div$ and $\sqrt{\ }$.

1.2: Polynomial equations

11. Prove Theorem 1.11 in the lecture notes, which says that $p : \mathbb{R} \to \mathbb{R}$ is a polynomial if and only if there exists $n \in \mathbb{N}$ such that $p^{(n)}(x) = 0$. ($p^{(n)}$ denotes the n^{th} derivative of p.)

    Hint: This is a biconditional proof. For the $(\Rightarrow)$ direction, use induction on the degree of p. For the $(\Leftarrow)$ direction, use induction on n. In either direction, you may use differentiation and/or integration rules you learn in calculus.

12. In class, we defined the degree of a constant polynomial like $p(x) = 3$ or $p(x) = -\sqrt{6}$ to be zero. There is a catch: the constant zero polynomial $p(x) = 0$ should not be said to have degree zero. The reason is that if this polynomial has degree zero, then Theorem 1.12 (which says that the degree of a product of two polynomials is the sum of the degrees of the polynomials) would be false.

    (a) If the degree of the constant zero polynomial $p(x) = 0$ is zero, give a specific counterexample "disproving" Theorem 1.12.

    (b) To make Theorem 1.12 work even if one or more of the polynomials is the zero polynomial, how do you think the degree of the polynomial $p(x) = 0$ should be defined? Explain

13. Consider the equation $x^3 + 3x^2 + 6x + 2 = 0$.

    (a) Make an appropriate substitution to transform this equation into a depressed cubic equation of the form
    $$y^3 + py + q = 0.$$

    (b) Compute the discriminant of this depressed cubic.

    (c) Use the method of del Ferro and Tartaglia to find a real root of the depressed cubic equation (go through all the steps; don't just use the formula in the box that we derived in the lecture notes).

    (d) What is the root of the original equation corresponding to the root you found in part (c)?

14. Let $f(x) = x^3 + px + q$. Verify the identity on page 47 of the lecture notes, which says that
$$\frac{1}{4} f\left(-\sqrt{\frac{-p}{3}}\right) f\left(\sqrt{\frac{-p}{3}}\right) = \frac{q^2}{4} + \frac{p^3}{27}.$$

15. Suppose $f(x) = x^3 + px + q$ has exactly two roots. Call the root where the graph of f is tangent to the x-axis the **repeated root** and the other root, where the graph crosses the x-axis, the **transverse root**.
    (a) Show that in this situation, the discriminant of f is zero.
    (b) Determine, with proof, which of the roots (the repeated one or the transverse one) is produced by applying the method of del Ferro and Tartaglia to f.

16. (a) Use the trig identity $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta$ (and perhaps other trig identities) to show that $\cos 3\theta$ can be written as $p(\cos\theta)$ for some polynomial p. What is $p(x)$?
    (b) Let $x = \cos 20^\circ$ (notice that if you can trisect a 60° angle, then x must be a constructible number). Write down a polynomial $f(x)$ with integer coefficients such that x is a root of this polynomial.
    Hint: use your answer to the previous HW question.

2.1: The natural numbers

17. Consider the binary operation $\oplus$ on $\mathbb{Z}$ defined by $a \oplus b = a + b - 1$.
    (a) Is the operation $\oplus$ associative?
    (b) Is the operation $\oplus$ commutative?
    (c) Does the operation $\oplus$ have an identity element? If so, what is it?
    (d) Does every element in $\mathbb{Z}$ have an inverse under the operation $\oplus$? If so, what is the inverse of a under $\oplus$?

2.2: The integers

18. Let R be a ring (in this class, "ring" means "commutative ring with 1") with additive identity 0 and multiplicative identity 1. Prove that the multiplicative identity element of R is unique. (Make sure that your proof is carefully written, and makes use only of the properties of rings laid out in Definition 2.8 of the lecture notes.)

    Hint: To prove uniqueness, suppose that there are two multiplicative identities (call them 1 and $1'$), and show they must be equal.

19. Let R be a ring with additive identity 0 and multiplicative identity 1. Prove that for all $x \in R$, $0x = 0$.

20. Let R be a ring with additive identity 0 and multiplicative identity 1. Prove that $-1(x) = -x$.

21. Let R and R' be rings. Define addition and multiplication on $R \times R'$ by $(x, y) + (x', y') = (x + x', y + y')$ and $(x, y)(x', y') = (xx', yy')$. Prove that this addition and multiplication makes $R \times R'$ into a ring.

2.3: The rational numbers

22. Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Prove that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$.

2.4: Divisibility

23. Prove statement (3) of Theorem 2.24 from the lecture notes, which says: If $a \mid b$ and $a \mid c$, then a divides any linear combination of b and c.

24. Prove statement (4) of Theorem 2.24 from the lecture notes, which says: if $a \mid b$ and $b \mid c$, then $a \mid c$.

25. Suppose $a, b \in \mathbb{Z}$ are such that $a \mid b$ and $b \mid a$. What conclusion can be drawn? Formulate your conclusion as a theorem, and prove it.

26. Let $a \in \mathbb{Z}$. Prove that either $8 \mid a^2$ or $8 \mid (a^2 - 1)$.

    Hint: By the Division Theorem, a has remainder $0, 1, 2$ or 3 when divided by 4. This suggests a proof by four cases.

    WARNING: This proof should be written without any reference to " $\mod$ "; in this class we have not introduced this language yet.

27. Prove that if $2^n - 1$ is prime, then n must be prime.

28. (EC) Prove or disprove: let $a, b \in \mathbb{Z}$. If $3 \mid (a^2 + b^2)$, then $3 \mid a$ and $3 \mid b$.

2.5: Euclidean algorithm

29. Use the Euclidean algorithm to find $\gcd(27182, 3141)$ and write this $\gcd$ as a linear combination of 27182 and 3141.

30. Use the Euclidean algorithm to find $\gcd(12906, 42905)$ and write this $\gcd$ as a linear combination of 12906 and 42905.

31. Prove Lemma 2.37 from the lecture notes, which says that if a and b are nonzero integers with $a \mid b$, then $\gcd(a, b) = |a|$.

32. Let $a \neq 0$ be an integer. Prove that $\gcd(a, a + 1) = 1$.

33. Let $a \in \mathbb{Z}$ be such that $|a| > 1$. Formulate and prove a statement about the value of $\gcd(a + 1, a - 1)$.

    Hint: To get an idea of what the statement should be, try some values of a.

34. Let $a, b \in \mathbb{Z}$ be nonzero. Prove that if a and b are relatively prime, then so are a^2 and b^2.

35. Suppose $a, b \in \mathbb{Z} - \{0\}$ and let $d = \gcd(a, b)$. Prove $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

36. (EC) Let $a, b \in \mathbb{Z} - \{0\}$. Prove or disprove: if $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

37. (EC)

    (a) Suppose $a \neq 0$ is an integer. Is there a reasonable definition of $\gcd(a, 0)$? If so, what is it? If not, why not?

    (b) Is there a reasonable definition of $\gcd(0, 0)$? If so, what is it? If not, why not?

38. Prove Lemma 2.41 from the lecture notes, which says that if p is prime and $a \in \mathbb{Z} - \{0\}$ is such that $p \nmid a$, then $\gcd(a, p) = 1$.

39. Prove Lemma 2.43 from the lecture notes, which says that if p is prime and $a_1, ...a_n \in \mathbb{Z}$ are such that
$$p \mid a_1 a_2 a_3 \cdots a_n,$$
then there is some j such that $p \mid a_j$.

40. Prove Lemma 2.44 from the lecture notes, which says that if $a, b, c \in \mathbb{Z}$ are such that $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

41. Suppose $A \subseteq \mathbb{Z}$ is a set with the following properties:
    - $0 \in A$;
    - $a \in A$ and $b \in A$ implies $a + b \in A$;
    - $a \in A$ implies $-a \in A$.

    Prove that there exists $n \in \mathbb{Z}$ such that $A = n\mathbb{Z}$.

42. (EC) Prove that an equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$, has a solution $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$.

43. (EC) Let $n \in \mathbb{N}$. Prove that there are n consecutive natural numbers, all of which are composite, by following these steps:

    (a) Prove that for any $k \in \{2, 3, ..., n + 1\}$, k divides $[(n + 1)! + k]$.

    (b) Use part (a) to prove the result.

44. (EC) Let $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. This set is a ring under the usual operations of $+$ and $\cdot$.

    (a) Is $\mathbb{Z}[\sqrt{2}]$ a field? Prove or disprove your answer.

    (b) Define $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ by $N(a + b\sqrt{2}) = a^2 - 2b^2$. Let $x, y \in \mathbb{Z}[\sqrt{2}]$; prove that N is multiplicative, i.e. $N(x)N(y) = N(xy)$.

    (c) Classify, with justification, the following elements of $\mathbb{Z}[\sqrt{2}]$ as a *unit*, *prime*, or *composite*:
$$7 \qquad\qquad 17 + 12\sqrt{2} \qquad\qquad 5 + 3\sqrt{2}.$$

45. (EC) The **least common multiple** of integers a and b, is the least positive integer $l = \text{lcm}(a, b)$ such that $a \mid l$ and $b \mid l$. Prove that for any integers a and b,
$$\gcd(a, b)\, \text{lcm}(a, b) = ab.$$

2.6: Congruence classes modulo n

46. Prove that the sum of any three consecutive integers must be divisible by 3.

    Hint: How must such a sum work in $\mathbb{Z}/3\mathbb{Z}$?

47. Let $n \in \mathbb{N}$.

    (a) Prove that $11 \mid n$ if and only if 11 divides the alternating sum of the digits in the base 10 representation of n (as an example, the alternating sum of the digits of 7432582 is $7 - 4 + 3 - 2 + 5 - 8 + 2$).

    (b) Use this fact to determine whether or not 11 divides 814518450.

48. Construct addition and multiplication tables for $\mathbb{Z}/11\mathbb{Z}$.

49. Let $m, n \in \mathbb{Z}$. Formulate a useful theorem of the form "$(a + m\mathbb{Z}) \subseteq (a + n\mathbb{Z})$ if and only if ...", and prove your theorem.

50. Suppose $a \equiv 7 \mod 9$ and $b \equiv 1 \mod 6$. Find $(a^2 + 2b) \mod 3$.

51. Consider the binary operation $\star$ on $\mathbb{Z}/n\mathbb{Z}$, where $n \geq 2$:

$$(a + n\mathbb{Z}) \star (b + n\mathbb{Z}) = \begin{cases} 1 + n\mathbb{Z} & \text{if } a \equiv b \mod 5 \\ 0 + n\mathbb{Z} & \text{if } a \not\equiv b \mod 5 \end{cases}$$

    (a) Is $\star$ well-defined when $n = 4$? Prove your answer.

    (b) Is $\star$ well-defined when $n = 5$? Prove your answer.

52. (EC) Is $\sqrt{\ }$ a well-defined function on $\mathbb{Z}/2\mathbb{Z}$? Is it well-defined on $\mathbb{Z}/3\mathbb{Z}$?

3.1: Theorems of Hippasus and Theatitus

53. Prove $\sqrt{3}$ is irrational, without using the Rational Roots Theorem or Corollary 3.6.

54. Prove that $\log_2 3$ is irrational.

55. Prove that the product of a nonzero rational number and an irrational number is irrational.

56. Find two irrational numbers x, y such that xy and $x + y$ are both rational.

57. (EC) Prove that there exist two irrational numbers a and b such that a^b is rational.

3.2: Real numbers

58. Use the IVT to prove that any polynomial with real coefficients whose degree is odd must have a real root.

    Note: In this and all other HW problems, you may use facts from pre-calculus and calculus.

59. Let $a, b \in \mathbb{R}$ with $a < b$, and suppose $f : [a, b] \to [a, b]$ is continuous. Prove f has a *fixed point*, i.e. a number $x \in [a, b]$ such that $f(x) = x$.

60. Use calculus to prove that $x^2 \geq 0$ for any real number x.

    Hint: optimization.

3.3: Complex numbers

61. Prove the four properties of conjugation described in Lemma 3.24 of the lecture notes.

62. If z is a complex number, what is true about $\overline{\overline{z}}$? Formulate your statement as a theorem, and prove it.

63. Prove Lemma 3.27 from the lecture notes, which says that if $z_1, z_2 \in \mathbb{C}$, then $|z_1 z_2| = |z_1||z_2|$.

64. (a) Compute $\frac{2+i}{3-2i}$, writing your answer as $x + iy$.
    (b) Find the reciprocal of $6 - 5i$, writing your answer as $x + iy$.
    (c) What is i^4? What about i^{13}? i^{-5}? Based on these observations, describe all possible values of i^n for $n \in \mathbb{Z}$, based on the value of $n \mod 4$.
    (d) Find the modulus and argument of $-7\sqrt{3} + 7i$.
    (e) If z has modulus 8 and argument $\frac{3\pi}{4}$, write z in $x + iy$ form.
    (f) Compute $(2 - 2\sqrt{3}\,i)^9$, writing your answer in $x + iy$ form.

65. (EC) Prove that there is no total ordering $\leq$ on $\mathbb{C}$ which has the following properties:

$$z \geq 0, w \geq 0 \Rightarrow (z + w \geq 0 \text{ and } zw \geq 0)$$

$$z \geq 0 \Rightarrow -z \leq 0$$

$$z \leq 0 \Rightarrow -z \geq 0$$

3.5: Complex roots, cubic equations and regular polygons

66. Find the three cube roots of $-8 - 8i$. Write them in $x + iy$ form.

67. Suppose $z = 2e^{i\pi/12}$. Let $w = z^6$. Find the other sixth roots of w, writing them in polar form.

68. (a) Compute $(2 + i)^3$ (by multiplying it out, not by using de Moivre's Theorem).
    (b) Find the three real roots of the polynomial $x^3 - 15x - 4$.
    Hint: What you did in (a) may come in handy.

69. Show that for every natural number $n \geq 1$, $\cos n\theta$ can be written as $p(\cos\theta)$, where p is a polynomial.

    Hint: induction on n, together with suitable trig identities (see HW problem # 16).

4.1: Polynomial rings (definition and basic properties)

70. Divide $x^3 + 1$ by $2x + 1$ in $\mathbb{Q}[x]$ (i.e. perform long division with remainder as in the Division Theorem).

71. Use the Euclidean algorithm (which works perfectly well in $F[x]$, you just have to make sure everything is a polynomial rather than an integer) to find

$$\gcd(x^4 + 2x^3 + x^2 + 1, x^2 + 2x + 4),$$

and write this gcd as a linear combination of $x^4 + 2x^3 + x^2 + 1$ and $x^2 + 2x + 4$. (Think of these polynomials as elements of $\mathbb{R}[x]$.)

72. Let F be a field.
    (a) Prove that $f \in F[x]$ is a unit if and only if f is a nonzero constant polynomial.
    (b) Let F be a field. Prove $F[x]$ is <u>not</u> a field.

73. (a) List <u>all</u> the elements of $\mathbb{F}_2[x]$ which have degree 3.
    (b) Let d be a positive integer. How many polynomials are there in $\mathbb{F}_p[x]$ which have degree d?
    (c) Let d be a positive integer. How many polynomials are there in $\mathbb{F}_p[x]$ which have degree at most d?

74. Let $f \in \mathbb{R}[x]$. Show that if $z \in \mathbb{C}$ is a root of f, so is $\overline{z}$. Use that fact to prove that the only irreducible polynomials over $\mathbb{R}$ are linear polynomials and quadratic polynomials with negative discriminant.

75. Show that $f(x) = x^2$ and $g(x) = x$ are the same *function* $\mathbb{F}_2 \to \mathbb{F}_2$. Are f and g the same polynomial in $\mathbb{F}_2[x]$?

76. Prove Theorem 4.21 from the notes, which says that if F is a field and $l \in F[x]$ is nonzero, then $F[x]/lF[x]$ is a field if and only if l is irreducible.

77. (a) Give a list of the cosets which comprise the set $\mathbb{F}_3[x]/(x^2 + 1)\mathbb{F}_3[x]$. How many are there?
    (b) Find an irreducible polynomial $l \in \mathbb{F}_2[x]$ of degree 4. List the cosets in the field $\mathbb{F}_2[x]/l\mathbb{F}_2[x]$. How many cosets are there?
    (c) Let p be prime and suppose $l(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n. How many cosets are there in $\mathbb{F}_p[x]/l\mathbb{F}_p[x]$?
    (d) Find a field with 9 elements and list its elements.

78. (EC) Let F be a field. Prove that there are infinitely many irreducible polynomials in $F[x]$.

4.2: Irreducibility tests

79. Prove or disprove each statement:
    (a) $x^4 + 3x^2 + 2$ is irreducible over $\mathbb{Q}$.
    (b) $6x^3 - 7x^2 + x - 6$ is irreducible over $\mathbb{Q}$.
    (c) $x^6 + 14x^3 - 35x + 70$ is irreducible over $\mathbb{Q}$.
    (d) $x^6 + 14x^3 - 35x + 70$ is irreducible over $\mathbb{R}$.
    (e) $x^2 + 1$ is irreducible over $\mathbb{F}_5$.

80. Let $p(x) = x^4 - 7x^2 - 30$.
    (a) Factor $p(x)$ into irreducibles over $\mathbb{C}$.
    (b) Factor $p(x)$ into irreducibles over $\mathbb{R}$.
    (c) Factor $p(x)$ into irreducibles over $\mathbb{Q}$.

81. Prove that the polynomial $x^3 + x^2 - 2x - 1$ (that we obtained at the end of Chapter 3 dealing with the regular $7-$gon) is irreducible.

    Hint: let $y = x + 2$ and use the substitution trick together with Eisenstein.

82. Find a monic, fourth-degree polynomial whose roots are $\pm\sqrt{2 \pm \sqrt{3}}$, and show this polynomial is irreducible over $\mathbb{Q}$.

5.1: Field extensions

83. Prove $\mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

84. Prove that $\sqrt{2}$ and $\sqrt{3}$ are each elements of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

85. Prove that for any $k \in \mathbb{Z}$, $\cos \frac{2\pi k}{n} \in \mathbb{Q}(\cos \frac{2\pi}{n})$.

    Hint: A previous HW problem may be useful.

5.2: Algebraic extensions

86. Prove Lemma 5.7 from the notes, which says that for any number field F and any α which is algebraic over F,
    (a) there is an irreducible polynomial $h \in F[x]$ such that $h(\alpha) = 0$; and
    (b) any two irreducible polynomials in $F[x]$ which have α as a root must have the same degree.

87. Let f be a minimal polynomial for α. Prove that for any polynomial $h \in \mathbb{Q}[x]$ with $h(\alpha) = 0$, $f \mid h$.

88. (a) Show that $1 + \sqrt{2} = \sqrt{3 + 2\sqrt{2}}$.

(b) Find a minimal polynomial for $\alpha = 1 + \sqrt{2}$ over $\mathbb{Q}$.
Note: When asked to find a minimal polynomial, you always have to justify that your answer is correct.

89. Find a minimal polyomial for $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}$.

90. Find a minimal polynomial for $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}(\sqrt{3})$.

91. Find a minimal polynomial for $\sqrt{3} + \sqrt{5}$ over $\mathbb{Q}(\sqrt{15})$.

92. (a) Write down the cyclotomic polynomial $\Phi_9(z)$.
    (b) Show that $\Phi_9(z)$ is irreducible over $\mathbb{Q}$.
    Hint: Use the substitution $y = z - 1$ in your answer to part (a), together with Eisenstein.
    (c) Determine, with proof, whether or not the regular 9-gon is constructible.

5.3: Linear algebra and field extensions

93. Prove Theorem 5.18 from the notes, which says that if F is a number field and $\alpha \in \mathbb{C}$ has degree n over F, then $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis of $F(\alpha)$ over F.

94. Prove that 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$.

95. Prove that 1 and $\sqrt{3}$ are linearly independent over $\mathbb{Q}(\sqrt{2})$.

96. Use the Dedekind Product Theorem to find (with proof) the dimension of, and a basis for, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

97. Prove $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

98. Find a minimal polynomial for $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ (prove that the polynomial is minimal), and explain how your answer to this question jives with your answer to Problem 96.

99. Let $a > 0$ be a rational number which is not a square (i.e. there is no $b \in \mathbb{Q}$ such that $b^2 = a$). Prove that $\sqrt[4]{a}$ has degree 4 over $\mathbb{Q}$.

100. Let $\alpha \in \mathbb{C}$ be a non-real root of the polynomial $x^3 - 3x + 4$. Find the inverse of $\alpha^2 + \alpha + 1 \in \mathbb{Q}(\alpha)$ explicitly, as a linear combination of the basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{Q}(\alpha)$.

5.4: Classical construction problems, revisited

101. Let α be the real root of the polynomial x^3+3x+1. Prove that α cannot be constructed with straightedge and compass.

102. (EC) Is it possible to construct a square whose area is equal to that of a given triangle (whose lengths are rational numbers)? Prove your assertion.

103. Prove that if $\gcd(p, q) = 1$ and if the regular p-gon and regular q-gon are both constructible, then the regular pq-gon is constructible.

104. (EC) In the notes, we proved that $\deg(\zeta_n/\mathbb{Q}) = \phi(n)$. What is the degree of $\cos \frac{2\pi}{n}$ over $\mathbb{Q}$? Prove your answer.

6.1: What is a homomorphism?

105. In each part of this question, you are given a function between algebraic structures. Determine, with proof, whether or not the given function is a homomorphism.

    (a) $\sigma : (\mathbb{Z}[x], +) \to (\mathbb{R}, +)$ defined by $\sigma(f) = f(2)$
    (b) $\sigma : (\mathbb{Q}[x], +) \to (\mathbb{Q}[x], +)$ defined by $\sigma(f)(x) = f(2x)$
    (c) $\sigma : (\mathbb{Q}[x], \circ) \to (\mathbb{Q}[x], \circ)$ defined by $\sigma(f)(x) = f(2x)$

106. Same directions as the preceding question:

    (a) $\sigma : (\mathbb{Z}/3\mathbb{Z}, +) \to (\mathbb{Z}/12\mathbb{Z}, +)$ defined by $\sigma(x + 3\mathbb{Z}) = (x + 12\mathbb{Z})$
    (b) $\sigma : (\mathbb{Z}/3\mathbb{Z}, +) \to (\mathbb{Z}/12\mathbb{Z}, +)$ defined by $\sigma(x + 3\mathbb{Z}) = (4x + 12\mathbb{Z})$
    (c) $\sigma : (\mathbb{Z}/12\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$ defined by $\sigma(x + 12\mathbb{Z}) = (x + 3\mathbb{Z})$

6.2: Isomorphisms and invariants

107. Let p be an odd prime. Prove that the function $\sigma : \mathbb{F}_p \to \mathbb{F}_p$ defined by $\sigma(x) = x^2$ is a field isomorphism.

108. Prove that if rings R and R' are isomorphic, then R is an integral domain if and only if R' is an integral domain. (In other words, prove that being an integral domain is an invariant of ring isomorphism.)

109. Prove that if rings R and R' are isomorphic, then R is a field if and only if R' is a field.

    Hint: Use part (4) of Lemma 6.8, which says that if $\sigma : R \to R'$ is a ring isomorphism, and $x \in R$ is a unit, then $\sigma(x)$ is a unit in R'.

110. Solve the system of congruences

$$\begin{cases} x & \equiv 12 \quad \text{mod } 17 \\ x & \equiv 11 \quad \text{mod } 19 \end{cases}$$

111. Consider the map $\phi : \mathbb{C} \to M_2(\mathbb{R})$ given by

$$\phi(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}.$$

Prove that ϕ is a ring isomorphism from $(\mathbb{C}, +, \cdot)$ to $(M_2(\mathbb{R}), +, \text{ matrix multiplication})$.

6.3: Ring homomorphisms

112. Let R be a ring. Determine, with proof, whether or not each given function is a ring homomorphism.

    (a) $\sigma : R \to R \times R$ defined by $\sigma(x) = (x, 0)$
    (b) $\sigma : R \to R \times R$ defined by $\sigma(x) = (x, x)$
    (c) $\sigma : R \times R \to R$ defined by $\sigma(x, y) = x$
    (d) $\sigma : R \times R \to R$ defined by $\sigma(x, y) = x + y$
    (e) $\sigma : R \times R \to R$ defined by $\sigma(x, y) = xy$

    Note: the product ring $R \times R$ has operations described in a previous HW problem.

113. Prove that if $\sigma : R \to R'$ is a ring homomorphism, then $\sigma(1) = 1$.

114. Let $\sigma : R \to R'$ be a ring homomorphism. Prove that if $x \in \ker(\sigma)$, then $xy \in \ker(\sigma)$ for any $y \in R$.

115. Let R be the set of continuous functions from $[0, 1]$ to $\mathbb{R}$, with the addition and multiplication operations being the usual addition and multiplication of functions (this set forms a ring; you do not need to prove this). Let $S \subseteq R$ be the set consisting of all $f \in R$ such that $f(\frac{1}{2}) = 0$. Prove $R/S \cong (\mathbb{R}, +, \cdot)$.

116. (EC) Let R be a ring. An **ideal** is a nonempty subset I of R with the following two properties:

    I **is closed under addition:** if $x, y \in I$, then $x + y \in I$;
    I **is closed under multiplication by any ring element:** if $x \in I$ and $r \in R$, then $rx \in I$.

    (a) If $\sigma : R \to R'$ is any ring homomorphism, prove that $\ker(\sigma)$ is an ideal of R.
    (b) Describe all the ideals in $\mathbb{Z}$.
    (c) Describe all the ideals of $\mathbb{R}$.
    (d) Prove that any non-constant ring homomorphism σ whose domain is $\mathbb{R}$ must be injective.

6.4: Automorphisms

117. (EC) Prove Theorem 6.19 from the lecture notes (the group properties of the set of automorphisms of a ring).

7.2: What is a group?

118. Are the following objects groups? If so, just write **Yes**. If not, write **No** and give a brief reason why (like "not associative" or "no identity", etc.).

    (a) $(\mathbb{R}, *)$ where $a * b = 2a + b$

(b) $(X, +)$ where X is the set of rational numbers whose denominator in lowest terms is a nonnegative power of 5, and $+$ is usual addition

(c) $(E, \star)$ where E is a set containing 0, and $a \star b = 0$ for any $a, b \in E$.

(d) $(G, +)$ where G is the set of continuous functions from $[0, 1]$ to $\mathbb{R}$, and $+$ is the usual addition on functions.

(e) $(\mathbb{Z}^3, \bullet)$ where $(a, b, c) \bullet (x, y, z) = (a + x, b + y, c + z + ay)$.

119. Let T be the collection of non-constant linear functions from $\mathbb{R}$ to $\mathbb{R}$ (examples of elements of T would be f and g where $f(x) = 2x + 5$ and $g(x) = 7 - x$). Prove that T forms a group under composition.

120. Prove the uniqueness of inverses in a group (i.e. that if h and k are both inverses of g, then $h = k$).

121. (EC) Let G be an abelian group. Prove that $(ab)^n = a^n b^n$ for any $n \in \mathbb{Z}$.

122. Let G be a finite group where $|G|$ is even. Prove that there is an element $g \in G$, other than the identity, such that $g = g^{-1}$.

123. In each part of this problem, you are given a group G and a subset $H \subseteq G$. Is H is a subgroup of G? If so, just write **Yes**. If not, write **No** and give a brief reason why (like "not closed under group operation " or "doesn't contain identity", etc.).

    (a) $G = (\mathbb{R}, +)$; $H = [0, \infty)$

    (b) $G = (\mathbb{R}, +)$; $H = \mathbb{Q}$

    (c) $G = ((0, \infty), \cdot)$; $H = \{1\}$

124. Same directions as the previous problem:

    (a) $G = (\mathbb{Z}, +)$; $H = 4\mathbb{Z}$

    (b) $G = GL(2, \mathbb{R})$, the set of 2×2 matrices with real entries and nonzero determinant (the group operation is matrix multiplication); H is the set of diagonal matrices in $GL(2, \mathbb{R})$

    (c) $G = GL(2, \mathbb{R})$; $H = \{M \in G : M = M^T\}$

125. Let G be a group. Suppose $w, x, y, z \in G$ satisfy the equation $xyz^{-1}w = e$.

    (a) Solve for y in terms of the other variables.

    (b) Solve for z in terms of the other variables.

126. Let H and K be subgroups of group G.

    (a) Is $H \cup K$ necessarily a subgroup of G? Prove your assertion.

    (b) Is $H \cap K$ necessarily a subgroup of G? Prove your assertion.

127. Let G and G' be groups, and let $\sigma : G \to G'$ be a group homomorphism. Prove that if H is a subgroup of G, then $\sigma(H)$ is a subgroup of G'.

128. Let G and G' be groups, and let $\sigma : G \to G'$ be a group homomorphism. Prove that σ is injective if and only if $\ker(\sigma) = \{e\}$.

129. (EC) Let G be a finite group, and let its elements be denoted $\{g_1, g_2, ..., g_n\}$. Let $x = g_1 g_2 \cdots g_n$; prove $x^2 = e$.

130. (a) Let G be a group. Is the map $\sigma : G \to G$ defined by $\sigma(g) = g^{-1}$ a homomorphism? Prove your assertion.
    (b) Let G be an abelian group. Is the map $\sigma : G \to G$ defined by $\sigma(g) = g^{-1}$ a homomorphism? Prove your assertion.

131. Suppose G is an abelian group and $\sigma : G \to G'$ is an isomorphism. Must G' be abelian? Prove your assertion.

132. Let G be a group, and let $g \in G$. The map $\varphi_g : G \to G$ defined by

$$\varphi_g(x) = gxg^{-1}$$

is called a **conjugacy** (or **conjugation** by g). Prove that conjugation by g is an automorphism of G.

7.3: Examples of groups

133. Let G_1 and G_2 be groups. Prove that $G_1 \times G_2$ is a group, where the group operation is defined coordinate-wise by

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2).$$

134. Give an explicit isomorphism between $(\mathbb{Z}/12\mathbb{Z}, +)$ and $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$ (and prove that your function is an isomorphism).

135. Prove that every group of order 2 is isomorphic to $(\mathbb{Z}/2\mathbb{Z}, +)$.

    Hint: Let G be a group of order 2. One of its elements is the identity, and one isn't. Use this to explain what the composition table of G must look like, and then write down an isomorphism between G and $(\mathbb{Z}/2\mathbb{Z}, +)$.

136. Prove that every group of order 3 is isomorphic to $(\mathbb{Z}/3\mathbb{Z}, +)$.

137. Perform the following computations in the dihedral group D_6, writing your final answer in the form fr^i for $i \in \{0, ..., 5\}$:

(a) f^7	(c) rf^2	(e) $rfrf$	(g) $rfr^3(r^2f)^{-1}fr^2$
(b) r^{-8}	(d) $(fr^4)^{-1}$	(f) $frfr$	(h) $fr^3ffr^{-2}fr^4$

138. (EC) Let $\sigma : G \to G'$ be a group isomorphism. Prove that if G is cyclic, then G' is cyclic.

139. Write a list of elements in the group $(\mathbb{Z}/20\mathbb{Z})^\times$. Is this group cyclic? Explain.

140. Describe the group of symmetries of a cube.

 Hint: To find the group of symmetries of a regular polygon and the group of symmetries of a regular tetrahedron, we looked at how the *vertices* of the object were permuted. For the cube, it may be easier to look at how the *faces* of the object are permuted, since there are less faces than vertices.

141. Let $F = \mathbb{Q}(\sqrt[4]{2}, i)$. Prove $Aut(F) \cong D_4$.

142. (EC) Describe the group of symmetries obtained by all the ways you can flip/rotate a twin mattress and put it back in a bed.

143. (EC) Let G be the additive group of the finite field $\mathbb{F}_4$. Find, with proof, another group we have studied that is isomorphic to G.

7.4: Permutation groups

144. Perform the following computations in the symmetric group, writing your answer in cycle notation:

 (a) $(1\,3\,2\,4)^{-1}$
 (b) $(5\,4\,2)^2$
 (c) $(1\,4\,2)(1\,3)(1\,2\,4)$
 (d) $(1\,5\,2\,4)(4\,1\,3\,5)e$
 (e) $(3\,5)(4\,3\,2)(2\,5\,1)$
 (f) $(1\,3\,6)^{-1}(3\,2\,4)(2\,5)$
 (g) $(1\,7)(2\,7)(3\,2)(5\,3)(1\,5)(1\,6)(6\,7)$
 (h) $(1\,2)(2\,3\,4)^2(1\,4)$

145. Find the order of each permutation:

 (a) $(1\,6\,2)$
 (b) $(1\,3\,7)(2\,4,\ 6\,8)$
 (c) $(1\,2)(3\,4)^{-1}(7\,9)$
 (d) $(1\,2\,3,\ 4,\ 5)(6\,7\,8)$

146. Determine all possible cycle structures for elements in $\mathcal{S}_5$. For each cycle structure, find the order of an element with that cycle structure, give the number of elements in $\mathcal{S}_5$ with that cycle structure, and determine whether permutations with that cycle structure are even or odd.

147. Repeat the instructions of the previous problem for $\mathcal{S}_8$.

148. True or false: there exists a positive integer N such that $(1\,2)$ can be written as the product of some number of 3-cycles in $\mathcal{S}_N$. Prove your answer.

149. True or false: there is a positive integer N such that in $\mathcal{S}_N$, there are three transpositions τ_1, τ_2 and τ_3 such that $\tau_1\tau_2\tau_3 = e$. Prove your answer.

150. (EC) What is the largest order of any element in $\mathcal{S}_{13}$? Explain.

7.5: Subgroups and cosets

151. Find all the left cosets, and all the right cosets of $H = \{e, (1\,2)\}$ in the dihedral group $\mathcal{A}_4$.

152. Let G be a group, and suppose $x \in G$ has order rs. What is the order of x^r? Prove your assertion.

153. Let $G = \mathcal{S}_5$ and let $H =< (1\,2\,3) >$. Compute the left coset $(1\,2)(4\,5)H$ and the right coset $H(3\,4\,5)$.

154. Prove that the only groups of order 4 are (up to isomorphism) $(\mathbb{Z}/4\mathbb{Z}, +)$ and the Klein 4-group V.

    Hint: Let G be a group of order 4. Analyze the possible orders of the elements of G.

155. Let p be a prime. Prove that every group of order p is isomorphic to $(\mathbb{Z}/p\mathbb{Z}, +)$.

156. (EC) Suppose abelian group G has an element g of order m and an element h of order n, where $\gcd(m, n) = 1$. Prove G contains an element of order mn.

157. Classify all groups of order 6 up to isomorphism.

158. (EC) Classify all groups of order 8 up to isomorphism.

159. (a) Find the remainder when 4^{1433} is divided by 131.
     (b) Find the remainder when 3^{1203} is divided by 42.

160. Prove that $\mathcal{A}_4$ has no subgroup of order 6.

161. Let G be a group where every element other than e has order 2. Prove G is abelian.

162. (EC) Suppose G is a group with no subgroups other than $\{e\}$ and G itself. Prove something about G.

    Note: I'm looking for something considerably stronger than "G is simple".

163. (EC) Prove that the only element in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order 2 is $(p-1) + p\mathbb{Z}$.

    Use this fact to prove **Wilson's Theorem**, which says that for any prime p, $(p-1)! \equiv (-1) \mod p$.

164. Suppose that group G contains elements of every order from 1 to 10. What is the smallest possible order of G?

165. List all the subgroups of the Klein 4-group V.

166. (EC) List all the subgroups of D_6. Which of them are normal?

167. Let $G = GL(2, \mathbb{R})$, the set of invertible 2×2 matrices with real entries (this forms a group under matrix multiplication). Let $H \leq G$ be the subgroup $< \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} >$. Find another group we have studied which is isomorphic to H.

7.6: Normal subgroups and quotient groups

168. Verify that $\mathcal{A}_3 \triangleleft \mathcal{S}_3$ by checking that all products of the form ghg^{-1} (where $g \in \mathcal{S}_3$ and $h \in \mathcal{A}_3$) lie in $\mathcal{A}_3$.

169. Let $H \leq \mathcal{S}_4$ be the set of permutations σ such that $\sigma(1) = 1$. Is H a normal subgroup of $\mathcal{S}_4$?

170. Find, with proof, a normal subgroup of $\mathcal{A}_4$ that has order 4.

171. Let G be a group. Define the **center** of G, denoted $Z(G)$, to be the set of elements of G that commute with every element of G. In other words,

$$Z(G) = \{h \in G : gh = hg \text{ for every } g \in G\}.$$

Prove that $Z(G) \triangleleft G$.

172. Let G be a group and let $A = G \times G$. Let $H \leq A$ be the subgroup $\{(g, g) : g \in G\}$.
   (a) Prove $G \cong H$.
   (b) Prove $H \triangleleft G$ if and only if G is abelian.

173. Prove that any subgroup H of G with $[G : H] = 2$ must be normal.

174. Prove that $< r >$ is a normal subgroup of D_n (here, r represents the smallest counterclockwise rotation in D_n).

8.2: Galois groups

175. Compute the following Galois groups (i.e. find a common group to which these are isomorphic, with justification):
   (a) $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}))$
   (b) $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(\sqrt{2}))$
   (c) $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}(i))$

176. Compute $Gal(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2}))$.

177. Compute the Galois group of the root field of $p(x) = x^4 - 16x^2 + 4$ over $\mathbb{Q}$ (this example was studied near the end of Section 8.1 in the notes).

178. Let $p \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5. Let $z \in \mathbb{C}$ be a root of p, and let $E = \mathbb{Q}(z)$.
   (a) Prove that any $\sigma \in Gal(E/\mathbb{Q})$ is determined completely by the value of $\sigma(z)$.
   (b) Prove that for any $\sigma \in Gal(E/\mathbb{Q})$, $\sigma(z)$ is a root of p.
   (c) Based on your answers to (a) and (b), what is the maximum possible order of $Gal(E/\mathbb{Q})$?

179. Prove or disprove: for any n, the dihedral group D_n is solvable.

8.3: Quintic equations, revisited

180. Prove that the Galois group of any irreducible quadratic polynomial in $\mathbb{Q}[x]$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}, +)$.

 Remark: The "Galois group of a polynomial" in $\mathbb{Q}[x]$ is $Gal(E/\mathbb{Q})$, where E is the root field of the polynomial.

181. Let $x^3 + px + q$ be an irreducible cubic polynomial, where $p, q \in \mathbb{Q}$, which has three distinct roots $x_1, x_2, x_3 \in \mathbb{C}$. Let E be the root field of this polynomial.

 (a) Show $\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$, where Δ is the discriminant defined in Chapter 1.

 (b) Prove that if Δ is a perfect square in $\mathbb{Q}$ (i.e. $\delta = \sqrt{\Delta} \in \mathbb{Q}$), then $Gal(E/\mathbb{Q}) \cong \mathcal{A}_3$.

 (c) Prove that if Δ is not a perfect square in $\mathbb{Q}$, then $Gal(E/\mathbb{Q}) \cong \mathcal{S}_3$.

182. (a) Find a irreducible cubic polynomial in $\mathbb{Q}[x]$ whose Galois group is isomorphic to $\mathcal{A}_3$.

 (b) Find a irreducible cubic polynomial in $\mathbb{Q}[x]$ whose Galois group is isomorphic to $\mathcal{S}_3$.