Math 302: Abstract Algebra
Problem List

1. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

   Note that Problem 1 is an "if and only if" problem. To show that (statement A) if and only if (statement B), you need to show that (statement A) implies (statement B) AND that (statement B) implies (statement A).

2. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

3. Let a and b be integers and $d = \gcd(a, b)$. If $a = da'$ and $b = db'$, show that $\gcd(a', b') = 1$.

4. Let n be a fixed positive integer greater than 1. If $a \bmod n = a'$ and $b \bmod n = b'$, prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$.

5. Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

6. Let n and a be positive integers and $d = \gcd(a, n)$. Show that the equation $ax \bmod n = 1$ has a solution if and only if $d = 1$. (To say that $ax \bmod n = 1$ has a solution means that there is at least one integer s such that $as \bmod n = 1$. In other words, think of x as the variable here.)

7. For every positive integer n, use induction to prove that a set with exactly n elements has exactly 2^n subsets (counting the empty set and the entire set).

8. Let $\mathbb{Z}$ be the set of integers. If $a, b \in \mathbb{Z}$, define $a \sim b$ if $ab \geq 0$. Is $\sim$ an equivalence relation on $\mathbb{Z}$? If so, prove that it is. If not, explain why not.

9. Let $\mathbb{Z}$ be the set of integers. If $a, b \in \mathbb{Z}$, define $a \sim b$ if $a + b$ is even. Prove that $\sim$ is an equivalence relation and determine the equivalence classes of $\mathbb{Z}$.

10. Suppose that $f : X \to Y$ and $g : Y \to Z$. Show that if f and g are both one-to-one, then so is the composition gf. Show that if f and g are both onto, then so is the composition gf.

11. In D_n, explain geometrically why a reflection followed by a reflection must be a rotation.

12. If r_1, r_2, and r_3 represent rotations in D_n and f_1, f_2, and f_3 represent reflections in D_n, determine whether $r_1 r_2 f_1 r_3 f_2 f_3 r_3$ is a rotation or a reflection.

13. Show that subtraction on the set of integers is not associative. (Thus, the integers under subtraction is not a group.)

14. Show that the group $GL(2, \mathbb{R})$ is non-abelian by producing a pair of matrices A and B such that $AB \neq BA$.

15. Show that the set $\{5, 15, 25, 35\}$ is a group under multiplication modulo 40. What is the identity of this group? Can you see any relationship between this group and $U(8)$? (Look more deeply here than the obvious. Try looking at the group tables for both groups.)

16. Suppose that a and b belong to a group and $a^5 = e$ and $b^7 = e$. Write $a^{-3}b^{-6}$ and $(a^3b^2)^{-2}$ without using negative exponents.

17. For any integer $n > 2$, show that there are at least two elements in $U(n)$ that satisfy $x^2 = 1$.

18. Prove that a group G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for *all* a and b in G.

19. If $a_1, a_2, \ldots, a_n$ belong to a group, what is the inverse of $a_1 a_2 \cdots a_n$?

20. For any elements a and b from a group and any integer n, prove that $(a^{-1}ba)^n = a^{-1}b^n a$.

21. Suppose the table below is a group table. Fill in the blank entries.

	e	a	b	c	d
e	e	–	–	–	–
a	–	b	–	–	e
b	–	c	d	e	–
c	–	d	–	a	b
d	–	–	–	–	–

22. Prove that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n if and only if n is a prime.

23. Let G be a finite group. Show that the number of elements x of G such that $x^3 = e$ is odd. Show that the number of elements of x in G such that $x^2 \neq e$ is even.

24. For $\mathbb{Z}_{12}$ and $U(10)$, find the order of the group and the order of each element of the group. What relation do you see between the orders of the elements of a group and the order of the group?

25. Suppose that a is a group element and $a^6 = e$. What are the possibilities for $|a|$? Provide reasons for your answer.

26. If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G. Give a short explanation why the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G.

27. Let G be a group, and let $a \in G$. Prove that $C(a) = C(a^{-1})$.

28. If a and b are distinct group elements, prove that either $a^2 \neq b^2$ or $a^3 \neq b^3$.

29. Suppose that a group contains elements a and b such that $|a| = 4$, $|b| = 2$ and $a^3b = ba$. Find $|ab|$.

30. Suppose G is a group that has exactly eight elements of order 3. How many subgroups of order 3 does G have?

31. Let a belong to a group and $|a| = m$. If n is relatively prime to m, show that a can be written as the nth power of some element of the group.

32. Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{12}$.

33. List the elements of the subgroups $\langle 3 \rangle$ and $\langle 15 \rangle$ in $\mathbb{Z}_{18}$. Now, suppose that G is a group and let a be a group element of order 18 in G. List the elements of the subgroups $\langle a^3 \rangle$ and $\langle a^{15} \rangle$.

34. Let a be an element of a group and let $|a| = 15$. Compute the orders of the following elements of G.

    (a) a^3, a^6, a^9, a^{12}

    (b) a^5, a^{10}.

    (c) a^2, a^4, a^8, a^{14}

35. If a cyclic group has infinite order, how many elements of finite order does it have? Please justify your response.

36. List the cyclic subgroups of $U(30)$.

37. In $\mathbb{Z}_{24}$ list all generators for the subgroup of order 8. Let $G = \langle a \rangle$ and let $|a| = 24$. List all generators for the subgroup of order 8.

38. How many subgroups does $\mathbb{Z}_{20}$ have? List a generator for each of these subgroups.

39. List all the elements of order 8 in $\mathbb{Z}_{8000000}$. How do you know your list is complete? Let a be a group element such that $|a| = 8000000$. List all elements of order 8 in $\langle a \rangle$. How do you know your list is complete?

40. Determine the subgroup lattice for $\mathbb{Z}_{12}$. (A subgroup lattice is a chart that includes all subgroups, and uses lines to indicated inclusions. See Chapter 4 in Gallian for an example.)

41. Let m and n be elements of the group $\mathbb{Z}$. Find a generator for the group $\langle m \rangle \cap \langle n \rangle$.

42. Suppose that G is a cyclic group and that 6 divides $|G|$. How many elements of order 6 does G have? If 8 divides $|G|$, how many elements of order 8 does G have? If a is one element of order 8, list the other elements of order 8.

43. Find the order of each of the following permutations.

    (a) (1357)

    (b) (12345)

    (c) $(a_1 a_2 \cdots a_k)$

44. Write the following permutations as a product of disjoint cycles.

    (a) (1235)(413)

    (b) (13256)(23)(46512)

45. What is the order of each of the following permutations?

    (a) (124)(357)

    (b) (124)(3567)

    (c) (1235)(24567)

    (d) (345)(245)

46. Show that a function from a finite set S to itself is one-to-one if and only if it is onto. Is this true when S is infinite?

47. How many elements of order 5 are there in S_7? (Hint: consider the cycle structure of such an element.)

48. Let G be a group of permutations on a set X. Let $a \in X$ and $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$. We call stab($a$) the *stabilizer of a in G* because it consists of all elements of G that leave a fixed. Prove that stab(a) is a subgroup of G.

49. Suppose that β is a 10-cycle. For which integers i between 2 and 10 is β^i also a 10-cycle? (Hint: Apply what you know about cyclic groups and consider the cycle structure of permutations of order 10.)

50. In S_3, find elements α and β such that $|\alpha| = 2$, $|\beta| = 2$, and $|\alpha\beta| = 3$. How does this relate to our theorem about the order of a product of cycles?

51. Given that β and γ are in S_4 with $\beta\gamma = (1432)$, $\gamma\beta = (1243)$, and $\beta(1) = 4$, determine β and γ.

52. Determine whether the following permutations are even or odd.

    a. (12345)
    b. (12)(134)(152)
    c. (1243)(3521)

53. Prove for all $n \geq 2$ that the subset of even permutations in S_n is a subgroup of S_n.

54. Prove that (1234) is not the product of 3-cycles.

55. Let $\beta = (1, 3, 5, 7, 9, 8, 6)(2, 4, 10)$. What is the smallest positive integer n for which $\beta^n = \beta^{-5}$?

56. Show that A_5 has 24 elements of order 5, 20 elements of order 3, and 15 elements of order 2.

57. Show that for $n \geq 3$, the center of S_n is trivial, i.e $Z(S_n) = \{\varepsilon\}$. (This problem can be hard to get started with. Scroll down for a hint if you would like one.)

    Hint for Problem 57: Since $n \geq 3$, there are at least 3 terms in the set A that is permuted by elements of S_n. Suppose that α is a nonidentity element in S_n, written in disjoint cycle notation. Explain why α must contain a cycle of the form $(a\, b \dots)$ for some $a, b \in A$. Now find another (very simple) element, based on distinct terms a, b, and c in A that does not commute with α. (Confirm that it does not commute.) Explain why this allows you to conclude why $Z(S_n) = \{\varepsilon\}$.

58. Find an isomorphism from the group of integers under addition to the group of even integers under addition. Prove that your map is an isomorphism.

59. Show that $U(8)$ is not isomorphic to $U(10)$.

60. Prove that the notion of group isomorphism is transitive. That is, if G, H, and K are groups and $G \approx H$ and $H \approx K$, then $G \approx K$.

61. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all g in G is an automorphism if and only if G is abelian.

62. For inner automorphisms φ_g, φ_h, and φ_{gh}, prove that $\varphi_g\varphi_h = \varphi_{gh}$. (Note: $\varphi_g\varphi_h$ and φ_{gh} are functions. To show that two functions f and g are equal, you must show that $f(x) = g(x)$ for all x in the domain of the functions.)

63. Let $G = \{a + b\sqrt{2} \,|\, a, b \text{ rational}\}$ and $H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \middle| \, a, b \text{ rational} \right\}$. Show that G and H are isomorphic under addition.

64. Let G be a group and let $g \in G$. If $z \in Z(G)$, show that the inner automorphism induced by g is the same as the inner automorphism induced by zg (that is, the mappings φ_g and φ_{zg} are equal).

65. Suppose that g and h induce the same inner automorphism of a group G. Prove that $h^{-1}g \in Z(G)$.

66. If G is a group, prove that $\text{Aut}(G)$ is a group. Do the details here: justify closure, show that the identity map is an automorphism, and show inverses are automorphisms.

67. Let a belong to a group G and let $|a|$ be finite. Let φ_a be the inner automorphism of G induced by a. Show that the order of φ_a in $\text{Aut}(G)$ divides the order of a in G (i.e. show that $|\varphi_a|$ divides $|a|$).

68. Let $H = \{0, \pm 3, \pm 6, \pm 9, \dots\} \leq \mathbb{Z}$. Use properties of cosets to decide whether the following cosets of H in $\mathbb{Z}$ are the same.

a. $11 + H$ and $17 + H$.

b. $-1 + H$ and $5 + H$.

c. $7 + H$ and $23 + H$.

69. Let $|a| = 30$. How many left cosets of $\langle a^4 \rangle$ in $\langle a \rangle$ are there? List them.

70. Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

71. Suppose that G is a finite group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime.

72. Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $[G : H] = [G : K][K : H]$.

73. Let G be a group of order pqr, where p, q, and r are distinct primes. If H and K are subgroups of G with $|H| = pq$ and $|K| = qr$, prove that $|H \cap K| = q$. (Hint: You need to show that $H \cap K$ is not trivial.)

74. Prove, by comparing orders of elements, that $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

75. How many elements of order 4 does $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ have? (Do not do this by examining the order of each element.) Explain why $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has the same number of elements of order 4 as does $\mathbb{Z}_{8000000} \oplus \mathbb{Z}_{400000}$. Generalize to the case $\mathbb{Z}_{4m} \oplus \mathbb{Z}_{4n}$.

76. The dihedral group D_n of order $2n$ ($n \geq 3$) has a subgroup of n rotations and a subgroup of order 2. Explain why D_n cannot be isomorphic to the external direct product of two such groups.

77. Show that if G and H are two cyclic groups, any isomorphism $\psi : G \to H$ is completely determined by the value of $\psi(g)$ when g is a generator of G. (In other words, show that if you know $\psi(g)$, then you can determine $\psi(g')$ for any other $g' \in G$.) With this in mind, how many isomorphisms are there from $\mathbb{Z}_{12}$ to $\mathbb{Z}_4 \oplus \mathbb{Z}_3$?

78. Suppose that φ is an isomorphism from $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ to $\mathbb{Z}_{15}$ and $\varphi(2,3) = 2$. Find the element in $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ that maps to 1.

79. Let $H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \,\middle|\, a, b, d \in \mathbb{R}, ad \neq 0 \right\}$. Note that H is a subgroup of $GL(2, \mathbb{R})$ (you do not need to prove this). Is H a normal subgroup of $GL(2, \mathbb{R})$?

80. Prove that if H has index 2 in G, then H is normal in G.

81. This problem will prove that the assumption that H is a normal subgroup of G is essential to the proof that G/H is a group.

    Let $H = \{(1), (12)(34)\}$ in A_4.

    (a) Show that H is not normal in A_4.

    (b) Referring to the table below, show that although $\alpha_6 H = \alpha_7 H$ and $\alpha_9 H = \alpha_{11} H$, it is not true that $\alpha_6 \alpha_9 H = \alpha_7 \alpha_{11} H$. Explain why this proves that the left cosets of H do not form a group under coset multiplication.

(In this table, the permutations of A_4 are designated as $\alpha_1, \alpha_2, \ldots, \alpha_{12}$ and an entry k inside the table represents α_k. For example, $\alpha_3 \alpha_8 = \alpha_6$.)

	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}
$(1) = \alpha_1$	1	2	3	4	5	6	7	8	9	10	11	12
$(12)(34) = \alpha_2$	2	1	4	3	6	5	8	7	10	9	12	11
$(13)(24) = \alpha_3$	3	4	1	2	7	8	5	6	11	12	9	10
$(14)(23) = \alpha_4$	4	3	2	1	8	7	6	5	12	11	10	9
$(123) = \alpha_5$	5	8	6	7	9	12	10	11	1	4	2	3
$(243) = \alpha_6$	6	7	5	8	10	11	9	12	2	3	1	4
$(142) = \alpha_7$	7	6	8	5	11	10	12	9	3	2	4	1
$(134) = \alpha_8$	8	5	7	6	12	9	11	10	4	1	3	2
$(132) = \alpha_9$	9	11	12	10	1	3	4	2	5	7	8	6
$(143) = \alpha_{10}$	10	12	11	9	2	4	3	1	6	8	7	5
$(234) = \alpha_{11}$	11	9	10	12	3	1	2	4	7	5	6	8
$(124) = \alpha_{12}$	12	10	9	11	4	2	1	3	8	6	5	7

(From Gallian "Contemporary Abstract Algebra" Seventh ed., p.107.)

82. Prove that a factor group of a cyclic group is cyclic.

83. What is the order of the element $14 + \langle 8 \rangle$ in the factor group $\mathbb{Z}_{24}/\langle 8 \rangle$?

84. Let G be a finite group and let H be a normal subgroup of G. Prove that the order of the element gH in G/H must divide the order of g in G.

85. Let H be a normal subgroup of G and let a belong to G. If the element aH has order 3 in the group G/H and $|H| = 10$, what are the possibilities for the order of a?

86. Let N be a normal subgroup of G and let H be a subgroup of G. If N is a subgroup of H, prove that H/N is a normal subgroup of G/N if and only if H is a normal subgroup of G.

87. Let N be a subgroup of a group G. We say that N is a *characteristic* subgroup of G if $\varphi(N) = N$ for all automorphisms φ of G. If N is a characteristic subgroup of G, prove that N is a normal subgroup of G.

88. Let $\mathbb{R}^*$ denote the group of nonzero real numbers under multiplication. Let $\mathbb{R}^+$ denote the group of positive real numbers under multiplication. Show that $\mathbb{R}^*$ is the internal direct product of $\mathbb{R}^+$ and the subgroup $\{+1, -1\}$.

89. In $\mathbb{Z}$, let $H = \langle 5 \rangle$ and $K = \langle 7 \rangle$. Prove that $\mathbb{Z} = H + K$. Is $\mathbb{Z}$ the internal direct product of H and K?

90. If φ is a homomorphism from G to H and σ is a homomorphism from H to K, show that $\sigma\varphi$ is a homomorphism from G to K. How are $\ker\varphi$ and $\ker\sigma\varphi$ related? If φ and σ are onto and G is finite, describe $[\ker\sigma\varphi : \ker\varphi]$ in terms of $|H|$ and $|K|$.

91. Prove that $(A \oplus B)/(A \oplus \{e\}) \approx B$. (Note that since $A \oplus \{e\} \approx A$, this gives a concrete way of understanding how external direct products and factor groups behave in a way similar to multiplication and division of numbers.)

92. Suppose that k is a divisor of n. Prove that $\mathbb{Z}_n/\langle k \rangle \approx \mathbb{Z}_k$. (Hint: Use the first isomorphism theorem. You will need to take care to confirm that your map is a homomorphism.)

93. Suppose that φ is a homomorphism from $\mathbb{Z}_{30}$ to $\mathbb{Z}_{30}$ and $\ker \varphi = \{0, 10, 20\}$. If $\varphi(23) = 9$, determine all elements that map to 9.

94. Suppose that there is a homomorphism φ from $\mathbb{Z}_{17}$ to a group G and that φ is not one-to-one. Determine φ.

95. How many homomorphisms are there from $\mathbb{Z}_{20}$ onto $\mathbb{Z}_8$? How many homomorphisms are there from $\mathbb{Z}_{20}$ to (but not necessarily onto) $\mathbb{Z}_8$?

96. If φ is a homomorphism from $\mathbb{Z}_{30}$ onto a group of order 5, determine the kernel of φ.

97. Prove that the mapping $\varphi : \mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z}$ given by $(a, b) \mapsto a - b$ is a homomorphism. What is the kernel of φ? Describe the set $\varphi^{-1}(3)$.

98. If K is a subgroup of G and N is a normal subgroup of G, prove that $K/(K \cap N)$ is isomorphic KN/N. (This is the Second Isomorphism Theorem.)

99. Give an example of a finite noncommutative ring. Give an example of an infinite noncommutative ring that does not have a unity.

100. The ring $\{0, 2, 4, 6, 8\}$ under addition and multiplication modulo 10 has a unity. What is it?

101. Find an integer n (other than 6) that shows that the rings $\mathbb{Z}_n$ need not have the following familiar properties of the ring of integers.

    (a) $a^2 = a$ implies $a = 0$ or $a = 1$.
    (b) $ab = 0$ implies $a = 0$ or $b = 0$.
    (c) $ab = ac$ and $a \neq 0$ imply $b = c$.

    Is the n you found prime?

102. Show that if m and n are integers and a and b are elements from a ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$. (Here, $m \cdot a$ means $a + \cdots + a$, m times.)

103. Show that a ring that is cyclic under addition is commutative.

104. Let a be a fixed element in a ring R. Let $S = \{x \in R \mid ax = 0\}$. Show that S is a subring of R.

105. Describe the elements of $M_2(\mathbb{Z})$ that have multiplicative inverses.

106. Let R be a commutative ring with unity and let $U(R)$ denote the set of units in R. Prove that $U(R)$ is a group under multiplication of R. (This group is called the *group of units of* R.)

107. Show that a unit of a ring divides every element of the ring.

108. Suppose that a and b belong to a commutative ring R with unity. If a is a unit of R and $b^2 = 0$, show that $a + b$ is a unit of R.

109. Suppose that there is an integer $n > 1$ such that $x^n = x$ for all elements x of some ring R. If m is a positive integer and $a^m = 0$ for some a, show that $a = 0$.

110. Show that $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $\mathbb{Z}$.

111. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

112. Describe all zero-divisors and units of $\mathbb{Z} \oplus \mathbb{Q} \oplus \mathbb{Z}$.

113. A ring element a is called an *idempotent* if $a^2 = a$. Prove that the only idempotents in an integral domain are 0 and 1.

114. Suppose that a and b belong to an integral domain. If $a^5 = b^5$ and $a^3 = b^3$, show that $a = b$.

115. Show that a finite commutative ring with no zero-divisors and at least two elements has a unity.

116. Give an example of an infinite integral domain that has characteristic 3.

117. Suppose that R is an integral domain in which $20 \cdot 1 = 0$ and $12 \cdot 1 = 0$. (Recall that $n \cdot 1$ means $1 + 1 + \cdots + 1$ with n terms.) What is the characteristic of R?

118. Let F be a field with characteristic 2 and more than two elements. Show that $(x+y)^3 \neq x^3 + y^3$ for some x and y in F.

119. Let F be a field of order 32. Show that the only subfields of F are F itself and $\{0, 1\}$.

120. Let $S = \{a + bi \mid a, b \in \mathbb{Z}, b \text{ is even}\}$. Show that S is a subring of $\mathbb{Z}[i]$, but not an ideal of $\mathbb{Z}[i]$.

121. If an ideal I of a ring R contains a unit, show that $I = R$.

122. Prove that the only ideals of a field F are $\{0\}$ and F itself.

123. Let R be a ring and let I be an ideal of R. Prove that the factor ring R/I is commutative if and only if $rs - sr \in I$ for all r and s in R.

124. Is the map $\varphi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ given by $\varphi(x) = 2x$ a ring homomorphism? Please show that it is or explain why it is not.

125. Let

$$S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}.$$

Show that $\varphi : \mathbb{C} \to S$ given by

$$\varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

is a ring isomorphism.

126. Determine all ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

127. Show that $(\mathbb{Z} \oplus \mathbb{Z})/(\langle a \rangle \oplus \langle b \rangle)$ is ring isomorphic to $\mathbb{Z}_a \oplus \mathbb{Z}_b$.

128. Let R and S be commutative rings with unity. If φ is an onto homomorphism from R to S and the characteristic of R is nonzero, prove that the characteristic of S divides the characteristic of R.