§1. Old Math 784 Test Problems: The Thinking Problems

1. Let α be an algebraic number, and let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. The minimal polynomial for α has degree n. Decide whether each of the following is true or false and give an appropriate justification for your answer. Note that an answer of "true" means that you believe the statement is true for all choices of α as above.

   (i) If β and γ are in R and β divides γ in R, then $N(\beta)|N(\gamma)$ in $\mathbb{Z}$.

   (ii) If β and γ are in R and $N(\beta)|N(\gamma)$ in $\mathbb{Z}$, then β divides γ in R.

   (iii) If $\beta \in R$, then $N(\beta) \in \mathbb{Z}$.

   (iv) If $\beta \in \mathbb{Q}(\alpha)$ and $N(\beta) \in \mathbb{Z}$, then $\beta \in R$.

   (v) If $N(\beta)$ is a rational prime, then β is irreducible in R.

   (vi) If β divides a unit in R, then β is a unit.

   (vii) If β divides an irreducible element of R and β is not a unit, then β is irreducible.

   (viii) If $N(\beta) = N(\gamma)$, then $\beta = \epsilon\gamma$ for some unit ϵ in R.

   (ix) The field conjugates of β all lie in $\mathbb{Q}(\alpha)$.

   (x) If $\sqrt{2} \in \mathbb{Q}(\alpha)$, then $\sqrt{2} \in R$.

   (xi) If $\sqrt{2} \in \mathbb{Q}(\alpha)$, then n is even.

   (xii) If $\sqrt{2} \in \mathbb{Q}(\alpha)$ and $\sqrt{3} \in \mathbb{Q}(\alpha)$, then $n > 2$.

   (xiii) If $\beta \in \mathbb{Q}(\alpha)$, then there is an odd integer d such that $d\beta \in R$.

   (xiv) If $\beta \in \mathbb{Q}(\alpha)$, then there is an even integer d such that $d\beta \in R$.

2. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-13})$. Since $-13 \equiv 3 \pmod 4$, $R = \mathbb{Z}[\sqrt{-13}]$. Observe that

$$(1+\sqrt{-13})(1-\sqrt{-13}) = 2 \cdot 7 \quad \text{and} \quad (2+\sqrt{-13})(2-\sqrt{-13}) = 17.$$

   (a) Explain why the norm of a non-zero non-unit element of R is at least 4.

   (b) Is 2 irreducible in R? Justify your answer.

   (c) Is 2 prime in R? Justify your answer.

   (e) Is R a UFD? Justify your answer using (b) and (c).

   (d) Is $2+\sqrt{-13}$ irreducible in R? Justify your answer.

   (f) Explain why the norm of an element of the ideal $(2, 1+\sqrt{-13})$ must be even.

   (g) Justify that $(2, 1+\sqrt{-13})$ is not principal. (Assume that it is (β). Note that both 2 and $1+\sqrt{-13}$ are in (β). What can you say about $N(\beta)$?)

   (h) Is R a UFD? Justify your answer using (g).

3. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{14})$. Observe that $4^2 - 14 = 2$ so that $N(4 \pm \sqrt{14}) = 2$. The number $15 + 4\sqrt{14}$ is a unit in R. Find a pair of positive integers $(x, y) \neq (4, 1)$ such that $x^2 - 14y^2 = 2$. Give specific integers x and y (not just a method for finding them).

4. (a) Prove that $\mathbb{Q}(\sqrt{5},\sqrt{7}) = \mathbb{Q}(\sqrt{5}+\sqrt{7})$.

   (b) Calculate $N_{\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}}\left(\sqrt{5}\right)$ and $Tr_{\mathbb{Q}(\sqrt{5}+\sqrt{7})/\mathbb{Q}}\left(\sqrt{5}\right)$.

   (c) Let α be a root of $x^3 - x - 1 = 0$. Explain why $\sqrt{5} \notin \mathbb{Q}(\alpha)$. The answer should be short, but try to state any results from class that you are using as clearly as possible.

5. If $n = 7$, then the product $n(n+2)$ is equal to 7 times a square. Find the next two positive integers n such that $n(n+2)$ is 7 times a square.

6. Let $\mathbb{Q}(\alpha)$ be an algebraic number field where α is a root of a cubic equation with coefficients in $\mathbb{Z}$. Suppose that $\{1, \alpha, \alpha^2\}$ is an integral basis for the ring R of algebraic integers in $\mathbb{Q}(\alpha)$.

   (a) Prove that $\{1, 1+\alpha, \alpha+\alpha^2\}$ is an integral basis for the ring R.

   (b) Prove that $\{1, 1+2\alpha, \alpha+\alpha^2\}$ is not an integral basis for the ring R.

7. Let α be a root of the irreducible polynomial $f(x) = x^3 - 3x^2 - 4$ (you do not need to explain why $f(x)$ is irreducible; this is given information).

   (a) What is the minimal polynomial of $1/\alpha$?

   (b) Compute $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^3)$ and $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^3)$.

   (c) Compute $\Delta(1, \alpha, \alpha^2)$.

8. The polynomial $f(x) = x^4 - x^3 + 1$ is irreducible over the rationals (you do not need to justify this). Let α denote a root of $f(x)$.

   (a) Show that $\Delta(1, \alpha, \alpha^2, \alpha^3) = 4^4 f(3/4)$.

   (b) Explain why $\{1, \alpha, \alpha^2, \alpha^3\}$ is an integral basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

9. Let α be a root of the irreducible polynomial $f(x) = x^8 - 2x^6 - 2$ (you do not need to explain why $f(x)$ is irreducible; this is given information). Let β be a root of $g(x) = x^4 - 2x^3 - 2$.

   (a) Why is $g(x)$ the minimal polynomial of β?

   (b) Must β be in $\mathbb{Q}(\alpha)$? Explain your answer.

   (c) Suppose $\beta \in \mathbb{Q}(\alpha)$. Must β be in the ring of algebraic integers in $\mathbb{Q}(\alpha)$? Explain (briefly).

   (d) Suppose $\beta \in \mathbb{Q}(\alpha)$. Compute $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$ and $\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)$.

   (e) Compute $\Delta(1, \alpha, \alpha^2, \ldots, \alpha^7)$.

10. Let N be a squarefree integer $\not\equiv 1 \pmod 4$ such that the ring R of algebraic integers in $\mathbb{Q}(\sqrt{N})$ is a UFD. Let p be an odd rational prime not dividing N.

    (a) Prove that if N is a square modulo p, then there exist integers x and y satisfying at least one of $p = x^2 - Ny^2$ and $-p = x^2 - Ny^2$.

    (b) Prove that if N is not a square modulo p, then there do not exist integers x and y satisfying either of $p = x^2 - Ny^2$ and $-p = x^2 - Ny^2$.

11. The ring R of algebraic integers in $\mathbb{Q}(\sqrt{-19})$ is not Euclidean but it is a unique factorization domain. (You may use this without proving it.) Consider an odd prime p such that -19 is a square modulo p.

    (a) Explain why there are non-negative rational integers u and v having the same parity (i.e., they are both even or both odd) such that $4p = u^2 + 19v^2$.

    (b) It is not the case that p itself can necessarily be written in the form x^2+19y^2 for some rational integers x and y. For example, the primes 5 and 61 cannot be expressed in the form x^2+19y^2 even though $1^2 \equiv -19 \pmod 5$ and $15^2 \equiv -19 \pmod{61}$ (so -19 is a square modulo 5 and modulo 61). Prove that p can necessarily be written in the form $5x^2 - 19xy + 19y^2$ for some non-negative rational integers x and y. (Hint: Consider $x = u$ and $y = (u+v)/2$ where u and v are from part (a).)

12. Suppose x, y and z are relatively prime rational integers (i.e., no prime divides all three of them) for which $x^2 + y^2 = z^3$. Let $R = \mathbb{Z}[i]$, where $i = \sqrt{-1}$.

    (a) Prove x, y and z are *pairwise* relatively prime (i.e., no prime divides two of them).

    (b) Show that x and y have opposite parity. In other words, show that one is even and one is odd.

    (c) Prove that if $r \in R$ and r divides both $x + iy$ and $x - iy$, then r is a unit.

    (d) Prove that there are rational integers u and v such that

    $$x = u(u^2 - 3v^2), \quad y = v(3u^2 - v^2), \quad z = u^2 + v^2.$$

    (Note: Any such x, y and z satisfies $x^2+y^2 = z^3$, but you do not need to justify this. In other words, if you completed this problem correctly, then you have found all the solutions to the Diophantine equation $x^2 + y^2 = z^3$.)

13. Let (x_n, y_n) denote the nth positive integral pair (x, y) satisfying $x^2 - 2y^2 = 1$ (ordered so that $x_1 < x_2 < \cdots$). Thus, for example, $(x_1, y_1) = (3, 2)$ and $(x_2, y_2) = (17, 12)$. Let p be a prime. Prove that

    $$x_p \equiv x_1 \pmod p \quad \text{and} \quad y_p \equiv y_1 \pmod p \quad \iff \quad p \equiv \pm 1 \pmod 8.$$

14. (a) It is a fact that if $p \equiv 1 \pmod{28}$, then -7 is a square modulo p. This can be shown by evaluating the Legendre symbol $\left(\dfrac{-7}{p}\right)$, but you do not need to justify this. Use this fact to prove that if $p \equiv 1 \pmod{28}$, then there are unique positive integers x and y such that $p = x^2 + 7y^2$.

    (b) Let n be an integer such that (i) $n \equiv 1 \pmod{28}$ and (ii) there are positive integers x and y satisfying $n = x^2 + 7y^2$. Must n be a prime? In other words, either prove that n is a prime or show that n may be composite.

15. Let B denote a positive integer. This problem concerns solutions to the equation $x^2 - 15y^2 = B$.

    (a) Suppose x and y satisfy $x^2 - 15y^2 = B$. Let $u = 4x - 15y$ and $v = 4y - x$. Prove that $u^2 - 15v^2 = B$ by direct substitution (express $u^2 - 15v^2$ in terms of x and y).

(b) Compute the fundamental unit in R, the ring of algebraic integers in $\mathbb{Q}(\sqrt{15})$. Show how the formulas for u and v in part (a) can be obtained by making use of this fundamental unit in R. (Think in terms of the norms of $x + \sqrt{15}y$ and the fundamental unit.)

(c) Prove that if x and y are positive in part (a), then $x/y > \sqrt{15}$.

(d) Suppose B is a positive integer for which $x^2 - 15y^2 = B$ has a solution in integers x and y. Prove that such a solution exists with

$$0 \leq y < \left(\frac{B}{2\sqrt{15}}\right)^{1/2}.$$

(Hint: When is $|v| < y$?)

(e) Suppose B is a positive integer ≤ 100. Find the set $S \subseteq \{1, 2, \ldots, 100\}$ for which the following holds: $x^2 - 15y^2 = B$ has a solution in integers x and y if and only if $B \in S$. Justify your answer.

16. Find (with proof) all integers x and y such that $y^2 + 1 = x^5$. (Note that the case that y is odd should be easy.)

17. Let α be an algebraic number with minimal polynomial $f(x)$ of degree m. Let $d(n)$ denote the number of divisors of a positive rational integer n.

(a) Prove that if p is a rational prime, then the ideal (p) is the product of $\leq m$ prime ideals in R.

(b) For n a rational integer, prove that the number of ideal divisors of (n) is bounded by $d(n)^m$.

(c) Suppose that $\alpha = \sqrt{-D}$ for some positive squarefree integer $D > 3$. Prove that if β and γ are in R and $(\beta) = (\gamma)$, then $\gamma = \pm\beta$. Discuss what happens in the cases that $D = 2$ and $D = 3$.

(d) Fix positive integers n and D with D squarefree and > 3. Show that the number of integer pairs (x, y) satisfying $x^2 + Dy^2 = n$ is $\leq 2d(n)^2$.

18. Suppose we wish to find integers x and y which satisfy $y^2 + 25 = 2x^3$. First, observe that y must be odd (this should be obvious). There are 2 cases one can consider, the case when 5 divides y and the case when 5 does not divide y. Do the second case. In other words, find all the solutions to $y^2 + 25 = 2x^3$ with $\gcd(10, y) = 1$. You should get one solution.

19. Let α be an algebraic number, and let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Let $f(x)$ be the minimal polynomial for α. Let p be a rational prime and suppose that $p \mid f(m)$ for some integer m and that $p^2 \nmid f(m)$. Let I be the ideal $(m - \alpha, p)$.

(a) Explain why I divides the principal ideals $(m - \alpha)$ and (p).

(b) Briefly justify that $N(m - \alpha) = f(m)$. (Note: $N(m - \alpha)$ is a norm of an *element* in R.)

(c) Why is $f(m)/(m - \alpha) \in R$?

(d) Show that 1 is not in the ideal I.

(e) Explain why the norm of the ideal I is p.

20. Let p be a rational prime, and suppose that there is a positive rational integer $a < p/2$ such that $a^2 \equiv -5 \pmod{p}$. For example, if $p = 7$, then $a = 3$; and if $p = 29$, then $a = 13$. Let R be the ring of integers in $\mathbb{Q}(\sqrt{-5})$.

    (a) Prove the following ideal factorization holds in R:

$$(p) = \big(a + \sqrt{-5}, p\big)\big(a - \sqrt{-5}, p\big).$$

    (b) What is the norm of the ideal $\big(a + \sqrt{-5}, p\big)$ in R? Justify your answer.

    (c) Is $\big(3 + \sqrt{-5}, 7\big)$ a prime ideal? Is $\big(13 + \sqrt{-5}, 29\big)$ a prime ideal? Justify your answers.

    (d) Is $\big(3 + \sqrt{-5}, 7\big)$ a principal ideal? Is $\big(13 + \sqrt{-5}, 29\big)$ a principal ideal? Justify your answers.

    (e) Is $\big(2 + \sqrt{-5}, 7\big)$ a principal ideal? Justify your answer.

21. Let α be an algebraic number, and let R be the ring of algebraic integers in $\mathbb{Q}(\alpha)$. Decide whether each of the following is true or false and give an appropriate justification for your answer. Note that an answer of "true" indicates that you believe the statement holds for every ring R as above.

    (i) If β and γ are in R, then $\beta^2 - \beta\gamma^3 + 5 \in R$.

    (ii) The ideal (2) is a prime ideal in R.

    (iii) The greatest common divisor of the ideals (4) and (6) is the ideal (2).

    (iv) If $\beta \in R$ with $\beta \neq 0$, then $N(\beta)/\beta \in R$.

    (v) If $\beta \in \mathbb{Q}(\alpha)$ with $\beta \neq 0$, then $N(\beta)/\beta \in R$.

    (vi) If $\beta \in R$, then the field conjugates of β all lie in $\mathbb{Q}(\alpha)$.

    (vii) If β is a non-unit in R that divides an irreducible element of R, then β is an irreducible element of R.

    (viii) If β is a non-unit in R that divides a prime element of R, then β is a prime in R.

    (ix) If I is an ideal in R and $N(I) = 1$, then $I = (1)$.

    (x) If I is an ideal in R and $N(I)$ is a square in $\mathbb{Z}$, then I is the square of some ideal in R.

22. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-47})$, and let I be the ideal in R generated by $(3 + \sqrt{-47})/2$ and 2. Thus,

$$I = \left(\frac{3 + \sqrt{-47}}{2}, 2\right).$$

    (a) Is I principal? (In other words, does there exist an $\alpha \in R$ such that $I = (\alpha)$?)

    (b) Let

$$J = \left(\frac{3 - \sqrt{-47}}{2}, 2\right).$$

    The product of the ideals I and J is a principal ideal (β) for some $\beta \in R$. Find such a β.

    (c) Compute the norm of the ideal I (in the ring R).

23. Let N be a squarefree rational integer $\equiv 3 \pmod 4$ such that the ring R of algebraic integers in $\mathbb{Q}(\sqrt{N})$ is a UFD. Let p be an odd rational prime not dividing N. Further suppose that N is a square modulo p.

    (a) Prove that if $p \equiv 1 \pmod 4$, then there exist integers x and y satisfying $p = x^2 - Ny^2$ but there do not exist integers x and y satisfying $-p = x^2 - Ny^2$.

    (b) Prove that if $p \equiv 3 \pmod 4$, then there exist integers x and y satisfying $-p = x^2 - Ny^2$ but there do not exist integers x and y satisfying $p = x^2 - Ny^2$.

    (c) Observe that $13 \equiv 1 \pmod 4$, 13 is a square modulo 3, and $13 = 5^2 - 3 \times 2^2$. Prove that there are infinitely many distinct pairs (x, y) of rational integers such that $13 = x^2 - 3y^2$.

24. For the following, $f(x) = x^3 - 10$ and α is a root (any root) of $f(x)$.

    (a) Find a polynomial $g(x)$ that has $3/(\alpha - 1)$ as a root.

    (b) Is $\{1, \alpha, \alpha^2\}$ an integral basis for the ring of algebraic integers in $\mathbb{Q}(\alpha)$? Justify your answer. (Hint: You should be able to see quickly that $\Delta(1, \alpha, \alpha^2)$ is not squarefree. This means that its value cannot be used in the obvious way to answer this question, regardless of the answer. I suggest instead thinking about what part (a) has to do with the question.)

25. Let R be the ring of integers in an algebraic number field $\mathbb{Q}(\alpha)$. In this problem, $N(x)$ is used to denote the norm of $x \in \mathbb{Q}(\alpha)$ over $\mathbb{Q}$. For each part, clearly indicate whether you believe the given statement is true or false. In this context, true means true for all choices of the variables satisfying the given conditions and false means false for some choice of these variables. If you believe the statement is true, provide a proof. If you believe the statement is false, provide a counter example. Note that one of the parts is true and one is false. This is information that is meant to help you, but saying something like, "This part is true because I know one of the parts is true and the other part is false" is NOT an acceptable justification. A correct justification of one part should be independent of the other part.

    (a) If a and b are in R and $N(a)$ and $N(b)$ are relatively prime in $\mathbb{Z}$, then the ideal (a, b) equals the ideal (1).

    (b) If a and b are in R and $N(a)$ and $N(b)$ are *not* relatively prime in $\mathbb{Z}$, then the ideal (a, b) does *not* equal the ideal (1).

26. The following concerns the Diophantine equation $x^2 + 13 = y^3$. The class number (the size of the class group) associated with the field $\mathbb{Q}(\sqrt{-13})$ is 2. In particular, the ring of integers R in $\mathbb{Q}(\sqrt{-13})$ is *not* a PID.

    (a) Suppose A is an ideal in R and A^3 is principal. Justify that A is necessarily a principal ideal in R. (Use that the class number is 2. You do not have to prove that the class number is 2.)

    (b) Suppose x_0 and y_0 are rational integers for which $x_0^2 + 13 = y_0^3$. Justify that $\gcd(y_0, 26) = 1$.

    (c) With the notation in part (b), justify that the ideals $\left(x_0 + \sqrt{-13}\right)$ and $\left(x_0 - \sqrt{-13}\right)$ are relatively prime.

    (d) Explain why there is a principal ideal $\left(a + b\sqrt{-13}\right)$ in R such that

$$\left(x_0 + \sqrt{-13}\right) = \left(a + b\sqrt{-13}\right)^3.$$

(e) Solve the Diophantine equation $x^2 + 13 = y^3$ (i.e., find with proof all integer pairs (x_0, y_0) such that $x_0^2 + 13 = y_0^3$.)

27. The class number for the field $\mathbb{Q}(\sqrt{-21})$ is 4. Using this information and material from the end of the course, explain why the equation $y^2 + 21 = x^{21}$ has finitely many solutions in integers x and y. (Note that I am not asking for the solutions.)

28. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{-26})$. The class number for the field $\mathbb{Q}(\sqrt{-26})$ is 6. You may use this information on the class number without proving it.

    (a) Let A, B and C be ideals in R with A and B principal, $B \neq (0)$ and $A = BC$. Using the definition of the product of two ideals, prove that C is principal.

    (b) Let A and C be ideals in R with A principal. Suppose $C^5 = A$. Using (a) and the definition of class numbers (but no lemmas from class), prove that C is principal.

    (c) Show that $y^2 + 26 = x^{17}$ has finitely many solutions in integers x and y. (Note that I am not asking for the solutions.)

§2. Old Math 784 Test Problems: The Proofs

29. Prove the theorem below. You should begin by considering $\beta \in \mathbb{Q}(\alpha)$ and using that there are $N(x)$ and $D(x)$ in $\mathbb{Q}[x]$ such that $\deg D(x) \leq n-1$, $D(\alpha) \neq 0$, and $\beta = N(\alpha)/D(\alpha)$. You do not need to prove such $N(x)$ and $D(x)$ exist. Note that the theorem is asserting that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ forms a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, so this is what you are trying to prove. In other words, don't use that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ as this would be circular reasoning. You should also not deduce the theorem below as a consequence of a more general or more difficult theorem.

    Theorem: *Let α be an algebraic number with minimal polynomial $f(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$. Every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely in the form $g(\alpha)$ where $g(x) \in \mathbb{Q}[x]$ with $\deg g(x) \leq n-1$.*

30. Prove the following theorem from class:

    Theorem: *Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{N})$. Then R is a Euclidean domain for $N = -1$, -2, -3, -7, and -11.*

31. Let B and C be ideals in the ring R of algebraic integers in an algebraic number field. Prove that $B|C$ if and only if $C \subseteq B$.

32. Two theorems are stated below. Using Theorem 1, prove Theorem 2.

    Theorem 1: *For any ideal B in R, there exists an ideal $C \neq (0)$ in R such that $BC = (a)$ for some $a \in \mathbb{Z}$.*

    Theorem 2: *Let B, C and D be ideals in R with $D \neq (0)$. If $BD = CD$, then $B = C$.*

33. Two theorems are stated below. You can use Theorem 3. Don't prove Theorem 4. Instead, I want to know how the proof of Theorem 4 begins. Tell me $N(A)N(B)$ distinct representatives for the $N(A)N(B)$ residue classes modulo AB. Note that you do not need to prove that the numbers you indicate are distinct or are representatives of the residue classes.

> **Theorem 3:** *If A and B are non-zero ideals in R, then there is a $\beta \in A$ such that $GCD\big((\beta), AB\big) = A$.*
>
> **Theorem 4:** *Let A and B be non-zero ideals in R. Then $N(AB) = N(A)N(B)$.*