Algebraic Number Theory Spring 2021
Homework List

April 19, 2021

`http://math.colorado.edu/~kstange/` click "Teaching"; also on canvas.

Advice: Please focus on the problems most appropriate to you (the ones you will learn something from). Aim to do at least 6 problems for a given due date. Many of these problems have solutions you can find in your texts or online. Give them a fair shake, but it's ok to learn solutions from elsewhere if you *make them your own* (by which I mean, learn them so you can authentically recreate them). (You are your own best guide to what helps you learn best.) When called upon, you can present anything that hasn't already been presented.

1 For Friday, January 29th.

1. Inspired by the first day, choose an interesting number theory question to dive deeper into and give a 5-10 minute presentation.
2. Show that $x^4 + y^4 = z^4$ has no nontrivial solutions. Hint: instead, show $x^4 + y^4 = z^2$ has no nontrivial solutions by writing it as $(x^2)^2 + (y^2)^2 = z^2$ and using the well-known parametrization of pythagorean triples. More specifically, show that if there's one solution, then there's another with smaller z (see the problem? this idea is called "infinite descent"). This exercise is elementary (it requires messing around with equations and parities), but not totally trivial. This case of FLT is originally due to Fermat himself.
3. Solve the Diophantine equation $x^3 - y^2 = 2$.
4. What is the appropriate "norm" function for $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$? What makes it appropriate?
5. Show that $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is a Euclidean domain, hence a UFD.
6. Classify the splitting possibilities for rational primes p as elements of $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. (Hint: this is a sixth root of unity.)
7. Prove that over an infinite field, no finite collection of proper subspaces can cover a vector space. What about finite fields?
8. Prove that $\mathbb{Z}[\sqrt{10}]$ is not a UFD (Hint: try factoring 6).
9. Find all the algebraic integers in $\mathbb{Q}(\sqrt{d})$. (Verify: in $\mathbb{Q}(i)$ you should get $\mathbb{Z}[i]$ and in $\mathbb{Q}(\sqrt{-3})$ you should get $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.)
10. Try to complete as much as you can of the Kummer/Lamé "proof" of FLT in the prime case, under the strong (and false!) assumptions that $\mathbb{Z}[\zeta_p]$ is a UFD and the only units are exactly $\pm\zeta_p^k$.

2 For Friday, February 12th.

1. Let V be a real two-dimensional vector space with v_1, v_2 as basis. Let W be a real two-dimensional vector space with w_1, w_2 as basis. Determine which of the following elements can be written as a simple tensor: $v_1 \otimes w_1 + v_2 \otimes w_2$, $4v_1 \otimes w_1 + 2v_1 \otimes w_2 + 2v_2 \otimes w_1 + v_2 \otimes w_2$. Prove it.

2. Use the proof that integrality is equivalent to finite generation of a certain module (Wed Jan 27) to find the minimal polynomial of $\sqrt[3]{2} + 1$. Verify it.

3. Prove that α is an algebraic integer if and only if its minimal polynomial has coefficients in $\mathbb{Z}$. (Note: This is Lemma 1.12 in Baker's Notes.)

4. In class (Mon Feb 1), we stumbled over the proof that if C/B and B/A are integral, then C/A is integral. Write out a nice proof of this.

5. We showed (Mon Feb 1) that if L/K is an extension of perfect fields, then the norm, trace and characteristic polynomial of $\alpha \in L$ are given in terms of the embeddings of L into $\overline{K}$. In this proof, we first assumed $L = K(\alpha)$. We left the general case as an exercise. Complete the proof. Hint: show the matrix for m_α on L is block diagonal, where the blocks are the corresponding matrix for $K(\alpha)$.

6. We have seen two definitions of the ring of algebraic integers of a number field. One is relative, as follows. Let $\mathcal{O}_K$ be the ring of integers of the number field K. Then the ring of integers $\mathcal{O}_L$ of an extension L/K is the integral closure of $\mathcal{O}_K$ in L. The other definition is global: the ring of integers $\mathcal{O}_L$ of L is the intersection of the ring of all algebraic integers (i.e. elements integral over $\mathbb{Z}$) with the field L. Prove that these define the same $\mathcal{O}_L$.

7. Suppose α and β are quadratic (i.e. degree 2 minimal polynomials). Determine the minimal polynomial of $\alpha + \beta$ in terms of that of α and β.

8. Show that $\sqrt{3}$ is not an element of $\mathbb{Q}(\alpha)$ where α is a fourth root of 2 (i.e. $\alpha^4 = 2$). Hint: start by using the minimal polynomial to compute trace. (Note: This is from Marcus, Chapter 2; more of a hint there.)

9. Find a cubic field $\mathbb{Q}(\alpha)$ where $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$. Possible method: modify the example we did in class Wed Feb 3 (computing the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$).

10. Consider the field K generated by a root α of minimal polynomial $x^3 - x^2 - 4x - 1$. Let $\beta = 1/(\alpha+1)$. Find the matrix representing multiplication by β, and its trace, norm and characteristic polynomial. Conclude that $\alpha + 1$ is invertible in $\mathcal{O}_K$.

11. We have defined the trace and norm maps for field extensions. Suppose we have a stack of field extensions $K \subseteq M \subseteq L$. What is the relationship between the maps $Tr_{L/M}$ and $Tr_{M/K}$ and $Tr_{L/K}$? What about the relationship between $N_{L/M}$, $N_{M/K}$ and $N_{L/K}$?

3 For Friday, February 26th.

1. Show that any commutative ring with identity has at least one maximal ideal (hint: use Zorn's lemma).

2. Show that in a Noetherian ring R, a subset is a fractional ideal if and only if it is a finitely generated R-submodule.

3. Show that if I and J are fractional ideals, so are IJ, $I \cap J$ and $I + J$.

4. Let $I = (1+i)\mathbb{Z}[i]$, an ideal of the Gaussian integers. Using the definition given in class before we proved the fractional ideals form a group,

$$I^{-1} = \{x \in \mathbb{Q}(i) : xI \subseteq \mathbb{Z}[i]\}.$$

   Find I^{-1} explicitly.

5. Do the same, but with the ideal $I = (3, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.

6. Find the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

7. Baker, Exercise (7) for Chapter 1.

8. Baker, Exercise (8) for Chapter 1.

9. Baker, Exercise (9) for Chapter 1.

10. Compute the discriminant of $\mathbb{Z}[\sqrt[3]{2}]$ in as many different ways as you can.

11. Baker, Exercise (11) for Chapter 1.

12. Compute the discriminant of α, i.e. $\mathrm{disc}(1, \alpha, \alpha^2, \alpha^3)$, where α has minimal polynomial $x^4 + ax + b$.

13. Suppose $\alpha_1, \ldots, \alpha_n$ is a basis for number field $K/\mathbb{Q}$ consisting entirely of algebraic integers, and suppose $\Delta = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$. Show that every algebraic integer of K can be expressed in the form $\frac{1}{\Delta}\sum_{i=1}^{n} b_i\alpha_i$, where $b_i \in \mathbb{Z}$.

4 For Friday, March 12th.

1. Allen Hatcher has a wonderful book called *The Topology of Numbers* (available in PDF on his website). Give a ten minute presentation on a topic, suitable for the class, of your choosing, from this book. (Warning: This is a rabbit hole. You may enjoy this rabbit hole. It is a very beautifully decorated rabbit hole. But it may be a dangerous rabbit hole. It is optional, of course.)

2. Learn what a Bhargava cube is and give a ten minute presentation on this topic. The best reference is the original reference: read up to the end of Section 2.3 in https://annals.math.princeton.edu/2004/159-1/p03.

3. Show that the class number of the Gaussian integers is 1, by finding the complete list of reduced primitive integral binary quadratic forms of discriminant -4.

4. Determine the full class group of $\mathbb{Q}(\sqrt{-14})$, including the class group structure. Find a corresponding quadratic form and ideal representative of each class. (You may be able to do this with quadratic forms – not sure how messy it gets – or you may wish to use the Minkowski bound we'll see in class.)

5. Let R be a Dedekind domain. Suppose $\mathfrak{p}$ and $\mathfrak{q}$ are distinct non-zero primes.

   (a) Show that $\mathfrak{p}$ and $\mathfrak{q}$ are coprime, i.e. $\mathfrak{p} + \mathfrak{q} = R$.

   (b) Show that for any positive exponents $s, t \in \mathbb{Z}$, $\mathfrak{p}^s$ and $\mathfrak{q}^t$ are coprime.

   (c) What aspect of this fails for a non Dedekind domain?

6. This example is due to Dedekind. Consider the field $K = \mathbb{Q}(\alpha)$ where α has minimal polynomial $x^3 + x^2 - 2x + 8$. In the ring of integers, one can verify that

   $$2 = (1 - (1/2)\alpha + (1/2)\alpha^2)(-3 + 2\alpha - \alpha^2)(-4 + (5/2)\alpha - (3/2)\alpha^2).$$

   Furthermore, each of these three elements has norm 2. From these facts, prove that K is non-monogenic (not just that $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$). Hint: Assume it is, and use Kummer's Theorem. Can one generalize this strategy?

5 For Monday, March 29th.

1. Consider the extension $K = \mathbb{Q}(\alpha)$ where α has minimal polynomial $\alpha^3 = \alpha + 1$. You may use the fact that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

   (a) Split the prime 23. By splitting, I mean break it into prime ideals, given explicitly, and determine which of these are equal and which are coprime.

(b) Verify the e_i, f_i and their expected relationship to n.

(c) Give the explicit maps from $\mathcal{O}_K$ to the finite fields corresponding to each prime.

2. (This is Marcus, Chapter 3, Exercise 9 among other places (it's very standard)). Let $K \subseteq L$ be number fields. Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ be ideals. One can naturally extend these ideals to ideals $\mathfrak{a}\mathcal{O}_L$ and $\mathfrak{b}\mathcal{O}_L$ of $\mathcal{O}_L$, by taking the ideal generated by their elements in the larger ring.

   (a) Show that if $\mathfrak{a}\mathcal{O}_L \mid \mathfrak{b}\mathcal{O}_L$, then $\mathfrak{a} \mid \mathfrak{b}$

   (b) Show that $\mathfrak{a} = \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$.

   (c) Which ideals $\mathfrak{C}$ of $\mathcal{O}_L$ satisfy $\mathfrak{C} = (\mathfrak{C} \cap \mathcal{O}_K)\mathcal{O}_L$?

3. Show that any ideal in a Dedekind domain can be generated by at most 2 elements. (There's a hint in Baker, Chapter 2 Exercise 4).

4. In class, we proved that when we split a prime $p \in \mathbb{Z}$ in a number field K, we have $\sum e_i f_i = n$ (see the details from the notes). State and prove a more general version of this for a relative extension $K \subseteq L$ of number fields. This will require generalizing definitions. (For reference, Marcus does this in Chapter 3, Theorem 21; you can approach this as an exercise or an expositional task depending how much you decide to depend on him.)

5. If you've done or understand the previous exercise, then explain and verify that e_i's and f_i's "multiply in towers".

6. In class we mentioned a variety of properties of dual lattices without proof (dual of dual is original lattice; how dual interacts with intersection and sum, etc.). Prove some or all of these.

7. Consider the field $K = \mathbb{Q}(\sqrt[3]{2})$. Pretend we don't already know that the ring of integers is $\mathbb{Z}[\sqrt[3]{2})$, but we do know $\operatorname{disc}(\mathbb{Z}[\sqrt[3]{2}]) = -108$.

   (a) Show that $(2) = (\sqrt[3]{2})^3$ and $(3) = (\sqrt[3]{2} + 1)^3$ in $\mathcal{O}_K$. (Hint: unlikely things can be units in a number ring, watch out.)

   (b) Explain why this determines the ring of integers.

   (c) What is the different ideal of $\mathcal{O}_K$?

8. Prove the following generalization of Minkowski's Convex Body Theorem: Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice. Let $S \subseteq \mathbb{R}^n$ be a bounded, convex, symmetric, and compact set. If $\operatorname{vol}(S) \geq 2^n \operatorname{vol}(\mathbb{R}^n/\Lambda)$ then there exists some $0 \neq v \in S \cap \Lambda$.

9. Prove the following generalization of Minkowski's Convex Body Theorem: Let $\Lambda \subset \mathbb{R}^n$ be a rank n lattice. Let $S \subseteq \mathbb{R}^n$ be a bounded, convex, symmetric set. Then, $|\Lambda \cap S| \geq \frac{\operatorname{vol}(S)}{2^n \operatorname{vol}(\mathbb{R}^n/\Lambda)}$. Can this statement be improved?

10. Suppose you plant a tree at every nonzero lattice point of $\mathbb{Z}^2$ within a radius of 13 from the origin. The trees are of diameter 0.16. You stand at the origin. Prove that you cannot see out of this forest. (Problem stolen from somewhere but I'm not sure where.)

11. More to be added (watch this space!) — Maybe?

6 For Monday, April 12th.

1. Baker, Exercise 4.16, page 92. Read Section 1.2 up to that exercise for the relevant definitions.

2. Let p be a prime. Find the limit of the sequence $1/(1+p^n)$ in $\mathbb{R}$ and in $\mathbb{Q}_p$. Are the limits rational? The same?

3. Let p be a prime. Prove that addition and multiplication are continuous as maps $\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p$.

4. Baker, Exercise 5.33 (page 128).

5. Baker, Exercise 5.36 (page 129).

6. Let p be a prime. Let $U_0 := \mathbb{Z}_p^*$. Let $\mathfrak{m} := p\mathbb{Z}_p$. Define $U_n := 1 + \mathfrak{m}^n$, which is a subset of U_0. Show the following isomorphisms of groups:

$$U_0/U_n \cong (\mathbb{Z}_p/\mathfrak{m}^n)^*, \quad U_n/U_{n+1} \cong \mathbb{Z}_p/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}.$$

   Note, U_1 are termed the *principal units*.

7. (Universal property for localization). Let R be a ring and S a multiplicatively closed subset. Let $h : R \to S^{-1}R$ be the map to the associated localization. The exercise is to show that $S^{-1}R$ satisfies the following universal property. For any other ring R' with a homomorphism $f : R \to R'$ for which $f(S) \subseteq (R')^*$, there is a unique homomorphism $g : S^{-1}R \to R'$ so that $f = g \circ h$.

8. Let R be a ring, and S be a multiplicatively closed subset. Define

$$\overline{S} := \{r \in R : ar \in S \text{ for some } a \in R\}.$$

   This is called the *saturation of* S.

   (a) Show that $\overline{S}$ is a multiplicatively closed subset containing S, and $\overline{S}^{-1}R \cong S^{-1}R$.

   (b) Find all multiplicative sets S such that $S^{-1}\mathbb{Z} = \mathbb{Q}$.

9. Let R be a ring, not necessarily an integral domain. In the absence of a fraction field, we can define localization more generally as follows. Let S be a multiplicatively closed subset (i.e. closed under multiplication and containing 1). Define a relation on $R \times S$ by

$$(a, b) \sim (c, d) \text{ if and only if } (ad - bc)s = 0 \text{ for some } s \in S.$$

Then $S^{-1}R$ is the set of equivalence classes. Write a/b for (a, b), and define addition and multiplication for equivalence classes as for fractions.

   (a) Check this is an equivalence relation and $S^{-1}R$ is a ring, and that $x \mapsto x/1$ is a homomorphism from R to $S^{-1}R$ (in class, only present the intersesting aspects of all these details).

   (b) Explain what you get for $S^{-1}R$ if you let S contain 0.

   (c) Localize $\mathbb{Z}/6\mathbb{Z}$ at $S = \{2, 4\}$. Is the map $R \to S^{-1}R$ given above injective?

   (d) Check that the correspondence between primes in $S^{-1}R$ and those of R not intersecting S (proved in class) is still valid.

10. Let R be a ring, not necessarily an integral domain. An element $x \in R$ is called *nilpotent* if some power $x^n = 0$. Show that the intersection of all prime ideals of R is the ideal consisting of all nilpotent elements. (Hints: This can be proven using localization as defined above. In particular, given a non-nilpotent x, we seek to find a prime not containing it. Localize at $S = \{x^k : k \geq 0\}$. What do you learn?)

7 For Monday, April 26th.

1. (Hensel's Lemma Practice)

   (a) Solve $x^3 - x - 2$ in $\mathbb{Q}_2$.

   (b) Let p be a prime. Let n not be divisible by p. Show that there is a unique n-th root of unity ζ in $\mathbb{Z}_p$ such that $\zeta \equiv 1 \pmod{p}$.

   (c) Let p be a prime. Find all solutions of $x^p - x = 0$ in $\mathbb{Z}_p$ and in $\mathbb{Q}_p$.

2. Solve the Diophantine equation $x^3 - 2y^3 = 1$. Hints: I haven't done this myself yet, but it looks like a good problem? Let θ be a cube root of 2. Then $-1 - \theta$ is a fundamental unit; we've also studied the discriminant -108 and ring of integers $\mathbb{Z}[\theta]$ for this field.

3. (Repeat from last time since no one presented it, but it's a useful exercise.) Let R be a ring, and S be a multiplicatively closed subset. Define

$$\overline{S} := \{r \in R : ar \in S \text{ for some } a \in R\}.$$

This is called the *saturation of* S.

(a) Show that $\overline{S}$ is a multiplicatively closed subset containing S, and $\overline{S}^{-1}R \cong S^{-1}R$.

(b) Find all multiplicative sets S such that $S^{-1}\mathbb{Z} = \mathbb{Q}$.

4. Let R be a ring with a multiplicatively closed set S. Let M be an R-module. The purpose of this exercise is to define localization of M, and show that it is actually a type of extension of scalars. To define the localization of M at S, denoted $S^{-1}M$, we use as underlying set (m, s), denoted m/s where $m \in M$ and $s \in S$, under the equivalence relation $m'/s' \sim m/s$ if and only if $(m's - ms')u = 0$ for some $u \in S$. This is based on the general definition of localization given in the last batch of exercises. If R is an integral domain, you can eliminate u from the definition.

(a) Show that if M is a ring extension of R, then this definition of $S^{-1}M$ coincides with the usual ring definition. (This is more of an observation than anything; not real work.)

(b) Show that $S^{-1}M \cong S^{-1}R \otimes_R M$. (Hint: Use the universal property of tensor product, i.e. start by giving a bilinear map $S^{-1}R \times M \to S^{-1}M$.)

5. (Some details of the $\sum fe = n$ proof from class.) Suppose B is a finite ring extension of A, both Dedekind domains. Let $S = A \setminus \mathfrak{p}$ for some prime ideal $\mathfrak{p}$. Let $\mathfrak{q}$ be a prime of B above $\mathfrak{p}$. Suppose that $\mathfrak{p}B = \prod \mathfrak{q}_i^{e_i}$.

(a) Show that $S^{-1}\mathfrak{q}$ is prime and lies above $S^{-1}\mathfrak{p}$.

(b) Show that $S^{-1}\mathfrak{p}B = \prod S^{-1}\mathfrak{q}_i^{e_i}$.

(c) Show that $B/\mathfrak{q}_i \cong S^{-1}B/S^{-1}\mathfrak{q}_i$.

(d) Show that $[B : A] = [L : K] = [B/\mathfrak{p}B : A/\mathfrak{p}]$ (Exercise 4.28 in Baker; hint there.)

6. More to be added (watch this space!)

TBA