Honors Algebra II, Courant Institute, Spring 2021

http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2021/HonorsAlgebraII.html

Check the class forum for corrections and hints

Assignment 11, due May 6 (before class starts).

Instructions

- Do not hand in a rough draft. Copy or type answers neatly and clearly. Points may be deducted for writing that is sloppy, has excessive cross-outs, or is hard to read.
- State facts precisely in clear language or notation. Put assertions in logical order. State clearly what the hypotheses and conclusions. Put the steps of an argument in logical order, including definitions. Points may be deducted for an incorrectly stated argument even if you seen to understand it. Clear mathematical exposition is an important goal for the class.
- Learn the Greek letters used in math. Learn their mathematical names and write them clearly.

Assigned Exercises, to hand in

1. Here is a way to verify that the integers in a quadratic number field form a ring.

   (a) Suppose $f(t)$ is a quadratic polynomial over $\mathbb{Q}$ and that $\mathbb{F}$ is the splitting field of f over $\mathbb{Q}$. Do not assume that f is monic or that the coefficients of f are integers. Show that $\mathbb{F} = \mathbb{Q}[\delta]$, where δ, where δ satisfies a monic quadratic polynomial equation with integer coefficients.

   (b) Show that if $\alpha \in \mathbb{F}$ satisfies a monic polynomial $g(\alpha) = 0$, $g \in \mathbb{Z}[t]$, then α satisfies a quadratic equation $\alpha^2 + a\alpha + b = 0$ with $a, b \in \mathbb{Z}$. *Hint.* If f factors over $\mathbb{Q}$ then f factors over $\mathbb{Z}$ (Gauss lemma).

   (c) Show that α is an integer in $\mathbb{F}$ (satisfies a monic integral polynomial) only if $\text{Tr}(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$.

   $$\text{Tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \ , \quad N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \ .$$

   (d) Express $\text{Tr}(\alpha + \beta)$ and $N(\alpha\beta)$ in terms of $\text{Tr}(\alpha)$, $\text{Tr}(\beta)$, $N(\alpha)$ and $N(\beta)$. (This is easy.)

   (e) Express $\text{Tr}(\alpha\beta)$ and $N(\alpha + \beta)$ in terms of $\text{Tr}(\alpha)$, $\text{Tr}(\beta)$, $N(\alpha)$ and $N(\beta)$. (Not as easy.)

   (f) Use parts (d) and (e) to show that the set of algebraic integers in $\mathbb{F}$ is a ring.

(g) (another fact) Show that any $\gamma \in \mathbb{F}$ may be written in the form $\gamma = r\alpha$ with $r \in \mathbb{Q}$ and α being an algebraic integer in $\mathbb{F}$.

2. Suppose $\mathbb{F}/\mathbb{Q}$ is a finite degree Galois extension. Let $R \subset \mathbb{F}$ be the ring of algebraic integers. You may assume (which we did not prove) that the set of algebraic integers forms a ring. Let $\sigma \in G$ be any element of the Galois group. An ideal $I \subset R$ is *prime* if $\alpha\beta \in I$ implies that $\alpha \in I$ or $\beta \in I$. An ideal I is *maximal* if there are no ideals "between" I and R. That means that if I' is a proper ideal with $I \subseteq I'$ then $I = I'$. Show that if $J = \sigma(I)$ then J is an ideal if and only if I is an ideal. Do the same for prime ideals and maximal ideals. Here, $\sigma(I)$ is the set of all elements of the form $\sigma(\alpha)$ for $\alpha \in I$.

3. This concerns prime factorization in the cyclotomic field $\mathbb{F} = \mathbb{Q}[\zeta_3]$, which includes a primitive third root of unity. Using the terminology in the text (which is not standard), let $R \subset \mathbb{F}$ be the ring of algebraic integers. If p is a rational prime and

   (a) Show that R is a euclidean domain.

   (b) Show that any prime ideal is a maximal ideal in a euclidean domain.

   (c) Show that if $I \subset R$ is a prime ideal, then $\sigma(I) = I$ for all $\sigma \in G$ (notation from Exercise 2) only if $I = (p)$ for a rational prime p or $I = (\zeta)$.

   (d) Show that the $(5) \subset R$ is a prime ideal. *Hint.* reduce mod 5.

   (e) Show that $I = (7)$ is not a prime ideal, but there is an ideal J with $I = J\overline{J}$ ($\overline{J} = \sigma(J)$, where σ is the non-identity element of G. That is, (7) is a product of distinct prime ideals.

   (f) Show that $(3) = I^2 = I \cdot I$ for some prime ideal I. [The terminology for this is that (3) is *ramified* while other primes are not. A prime ideal in $\mathbb{Z}$ (or a rational prime number) is *unramified* if it remains prime in R or if it is a product of distinct prime ideals in R. This exercise shows that 3 is ramified while the other ideals are not.]

4. Suppose that $\mathbb{F} \subset \mathbb{C}$ is a finite degree extension of $\mathbb{Q}$ and $[\mathbb{F} : \mathbb{Q}] > 2$. Show that the algebraic integers in $\mathbb{F}$ do not form a discrete lattice.

5. Exercise 1.1 from Chapter 13.

6. Exercise 1.4 from Chapter 13.

7. Exercise 2.1 from Chapter 13.

8. Exercise 4.1 from Chapter 13.