HW #3

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Reading Homework. Try Exercises A.2, A.3, A.5 in the textbook. Read their solutions in the back.

Question 1.

(1) Let K be a field. Show that $K[X]$ is a Dedekind domain.

Hint. You can use that $K[X]$ is a UFD.

(2) Let K be a field. Show that $K[X, Y]$ is **not** a Dedekind domain.

(3) Let R be a Dedekind domain, and let $r \in R$ be a non-zero element. Show that the ring

$$R\left[\frac{1}{r}\right] := \left\{\frac{a}{r^n} \in \mathrm{Frac}(R) \ : \ a \in R, n \geq 0\right\}$$

is also a Dedekind domain.

Question 2. Let $K = \overline{K}$ be an algebraically closed field, and let $f(X) \in K[X]$. We are interested in when the ring[1]

$$R := K[X, Y]/(Y^2 - f(X))$$

is a Dedekind domain. It is clear that $f(X)$ needs to be a non-square for R to be an integral domain, which we assume.

(1) If R is a Dedekind domain, show that the following condition is satisfied:

$$(\star) \qquad \text{There is no element } \alpha \in K \text{ such that } 2f(\alpha) = \frac{df}{dX}(\alpha) = 0.$$

Hint. Suppose that there is such an α. Let $\beta \in K$ be such that $\beta^2 = f(\alpha)$. Show that $\frac{Y-\beta}{X-\alpha} \in \mathrm{Frac}(R)$ is integral over R, and that this element is not an element of R. **Treat the cases** $\mathrm{char}\, K \neq 2$ **and** $\mathrm{char}\, K = 2$ **separately.**

(2) Show that, when $\mathrm{char}\, K \neq 2$, $(\star)$ is just merely requiring that $f(X)$ is a square-free polynomial. Why is $(\star)$ a much more stringent condition when $\mathrm{char}\, K = 2$?

(3) If R satisfies $(\star)$, show that R is a Dedekind domain.

Hint. If $\mathrm{char}\, K = 2$, show that R is, as an abstract ring, isomorphic to $K[X]$ (!). If $\mathrm{char}\, K \neq 2$, mimic the computation of ring of integers for quadratic fields.

[1] This is the analogue of the "quadratic field" case for $K[X]$ instead of $\mathbb{Q}$.

Question 3. Recall that, in class, we showed that the unique prime factorization of numbers does not hold for $\mathbb{Z}[\sqrt{-5}]$, because of the identity

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

We also saw how this is salvaged by considering ideals. The key was that there are prime ideals of the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ that are not principal. See Example 2.10 for a detailed explanation.

We will call the identity of the above form a **counterexample to unique prime factorization of numbers** for $R = \mathbb{Z}[\sqrt{-5}]$. Namely, it is an identity of the form $ab = cd$ where a, b, c, d are irreducible elements of R such that a or b is not equal to c or d even up to multiplication by a unit.

Here comes the task: go to LMFDB (`https://lmfdb.org`), and in the "Number fields" section, choose your favorite number field K which is

- not $\mathbb{Q}(\sqrt{-5})$,
- and has a non-trivial class group (i.e., the "Class group" column is not "trivial").

For such a K, find a counterexample to unique prime factorization of numbers for $\mathcal{O}_K$, as defined above. Explain also why this is salvaged by the unique factorization of prime ideals, just as we did in class.