Introduction to Algebraic-Geometric Codes **Spring 2019**

Exercise 1

Publish Date: February 28, 2019 *Due Date: March 7, 2019*

Exercise 1.1 *Let $I, J \triangleleft R$. Are the following sets ideals? If not, give a counter example and define the smallest ideal that contain it.*

(a) R^*.

(b) $I \cup J$.

(c) $I \cap J$.

(d) $I + J := \{a + b \mid a \in I, b \in J\}$.

(e) $I * J := \{ab \mid a \in I, b \in J\}$.

(f) *If I, J are prime, which of the previous is a prime ideal?*

(g) *If I, J are maximal, which of the previous is a maximal ideal?*

(h) *If I, J are principal, which of the previous is a principal ideal?*

Exercise 1.2 *Let $D \in \mathbb{Z}$ be a number that is not square. We define*

$$\mathbb{Z}[\sqrt{D}] = \{a + \sqrt{D}b \mid a, b \in Z\}.$$

Note that $\mathbb{Z}[\sqrt{D}]$ is a ring (no need to prove). For $\alpha = a + \sqrt{D}b \in \mathbb{Z}[\sqrt{D}]$, define $\overline{\alpha} = a - \sqrt{D}b \in \mathbb{Z}[\sqrt{D}]$. Then define $N : \mathbb{Z}[\sqrt{D}] \to Z$ as follows:

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - Db^2$$

Proof that, for $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$

(a) *The map $\alpha \in \mathbb{Z}[\sqrt{D}] \to \overline{\alpha} \in \mathbb{Z}[\sqrt{D}]$ is a ring homomorphism.*

(b) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(c) $N(\alpha) = 0 \iff \alpha = 0$

(d) $N(\alpha) = \pm 1 \iff \alpha \in \mathbb{Z}[\sqrt{D}]^*$

(e) $\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$. *Show that the other direction is not necessarily true*

Exercise 1.3 *Let S be a set of polynomials with coefficient in $\mathbb{Z}$ that have no linear term (that is, that the coefficient of x is 0).*

(a) *Prove that $S \subset \mathbb{Z}[x]$ is a subdomain.*

(b) *Prove that $x^6 \in S$ can be written as a product of irreducibles in two different ways, deduce that S is not a UFD.*

(c) *Find a polynomial that is irreducible in S but is not prime in S.*

Exercise 1.4 *Let R and S be rings, and $f : R \to S$ be a homomorphism.*

(a) *State which of the following is true, and which is false. No proof needed.*

(i) *Let $I \lhd R$ then $f(I)$ is an ideal in S.*

(ii) *Let $J \lhd S$ then $f^{-1}(J)$ is an ideal in R.*

(iii) *Let $I \lhd R$ be a prime ideal, then $f(I)$ is a prime ideal in S.*

(iv) *Let $J \lhd S$ be a prime ideal, then $f^{-1}(J)$ is a prime ideal in R.*

(v) *Let $I \lhd R$ be a maximal ideal then $f(I)$ is a maximal ideal in S.*

(vi) *Let $J \lhd S$ be a maximal ideal then $f^{-1}(J)$ is a maximal ideal in R.*

(vii) *Let $I \lhd R$ be a principal ideal then $f(I)$ is a principal ideal in S.*

(viii) *Let $J \lhd S$ be a principal ideal then $f^{-1}(J)$ is a principal ideal in R.*

(b) *Characterize the ideals in R/I, i.e, describe the ideals in R/I using only ideals in R.*