Math 562 — Spring 2014
Homework 4 — Drew Armstrong

Problems on Integers.

1. $\mathbb{Z}[\sqrt{-1}]$ is Euclidean. Historically, the first Euclidean domain considered (by Gauss) beyond $\mathbb{Z}$ and $\mathbb{Q}[x]$ was the ring of Gaussian integers:

$$\mathbb{Z}[\sqrt{-1}] := \{a + b\sqrt{-1} : a, b \in \mathbb{Z}\}.$$

(a) We can think of $\mathbb{Z}[\sqrt{-1}]$ as a "square lattice" in the complex plane $\mathbb{C}$. Draw it.

(b) Given $0 \neq \beta \in \mathbb{Z}[\sqrt{-1}]$ we can think of the principal ideal $(\beta) = \{\mu\alpha : \mu \in \mathbb{Z}[\sqrt{-1}]\}$ as a "square sublattice" of $\mathbb{Z}[\sqrt{-1}]$. Draw the ideal $(2 + \sqrt{-1})$.

(c) Consider the "size function" $\sigma : \mathbb{Z}[\sqrt{-1}] \to \mathbb{N}$ defined by $\sigma(a+b\sqrt{-1}) := |a+b\sqrt{-1}|^2 = a^2 + b^2$. Given any $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ with $\beta \neq 0$, show that we can find an element $\mu\beta$ of the lattice (β) such that $\sigma(\alpha - \mu\beta) < \sigma(\beta)$. [Hint: α lies in some square of the square lattice (β).]

(d) Conclude that $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain with size function σ.

2. $\mathbb{Z}[\sqrt{-3}]$ is not Euclidean. Now consider the ring

$$\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

(a) Define the "norm function" $N : \mathbb{Z}[\sqrt{-3}] \to \mathbb{N}$ by

$$N(a + b\sqrt{-3}) := |a + b\sqrt{-3}|^2 = a^2 + 3b^2.$$

Prove that for all $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

(b) Prove that $\alpha \in \mathbb{Z}[\sqrt{-3}]$ is a unit if and only if $N(\alpha) = 1$. [Hint: Use part (a).]

(c) Use part (b) to show that $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$. [Hint: If $a^2 + 3b^2 = 1$ for $a, b \in \mathbb{Z}$ then we must have $b = 0$.]

(d) Prove that there is no $\alpha \in \mathbb{Z}[\sqrt{-3}]$ such that $N(\alpha) = 2$. [Hint: $\sqrt{2}$ is not an integer.]

(e) If $N(\alpha) = 4$, show that α is irreducible in $\mathbb{Z}[\sqrt{-3}]$. [Hint: If α is **reducible** then by part (a) it has a factor of norm 2. Then use part (d).]

(f) Finally, note that we can factor $4 \in \mathbb{Z}[\sqrt{-3}]$ in two ways:

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Show that 2 and $1 \pm \sqrt{-3}$ are **irreducible**, but that 2 is **not associate** to $1 \pm \sqrt{-3}$. We conclude that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, hence it is not a PID, hence it is not Euclidean. [Hint: Use parts (c) and (e).]

Problems on Polynomials Over a Field.

3. Evaluating a Polynomial. Let $K \subseteq L$ be a field extension. That is, let K, L be fields such that L is a subring of L. For all $\alpha \in L$ we define a function $\mathrm{ev}_\alpha : K[x] \to L$ by

$$\sum_k a_k x^k \mapsto \sum_k a_k \alpha^k.$$

We will often write $f(\alpha) := \mathrm{ev}_\alpha(f(x))$ for simplicity.

(a) Prove that $\mathrm{ev}_\alpha : K[x] \to L$ is a ring homomorphism.

(b) Since $K[x]$ is a PID, the kernel of the evaluation is generated by a single polynomial

$$\ker(\mathrm{ev}_\alpha) = (m_\alpha(x)) = \{m_\alpha(x)f(x) : f(x) \in K[x]\}.$$

We call $m_\alpha(x)$ the minimal polynomial of α over K. (It is unique up to a nonzero constant multiple.) Prove that $m_\alpha(x)$ is irreducible. [Hint: Assume that $m_\alpha(x) = f(x)g(x)$. Evaluate at α to conclude that $f(\alpha) = 0$ or $g(\alpha) = 0$. Then what?]

(c) The image of the evaluation $K[\alpha] := \mathrm{im}\,(\mathrm{ev}_\alpha)$ is called "K adjoin α". It is the smallest subring of L that contains K and α. If ev_α is not injective, prove that $K[\alpha]$ is a field. [Hint: Show that the ideal $(m_\alpha(x))$ is maximal.]

4. Counting Roots. Let $K \subseteq L$ be a field extension and consider a polynomial $f(x) \in K[x]$. We say that $\alpha \in L$ is a root of $f(x)$ if $f(\alpha) = 0$. (Recall the evaluation morphism from Problem 3.) You showed on HW1 that

$$\alpha \in L \text{ is a root of } f(x) \quad \Longleftrightarrow \quad (x - \alpha)|f(x) \text{ in } L[x].$$

If $f(x) \in K[x]$ has degree n, prove that f has at most n distinct roots in any field extension. [Hint: Use induction on n. Recall that $\deg(fg) = \deg(f) + \deg(g)$.]