Math 562 Homework 4

Spring 2014 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:

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

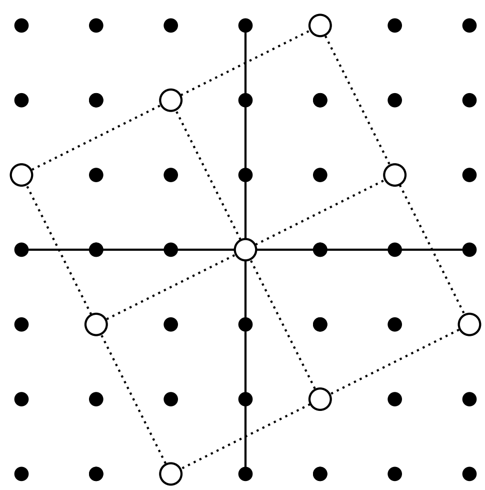
(a) We can think of $\mathbb{Z}[\sqrt{-1}]$ as a "square lattice" in the complex plane $\mathbb{C}$. Draw it.

(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.

Proof. For parts (a) and (b) consider the following picture.



The vertices are the Gaussian integers in the complex plane. The white vertices are the elements of the principal ideal

$$\begin{aligned}(2 + \sqrt{-1}) &= \{(2 + \sqrt{-1})(a + b\sqrt{-1}) : a, b \in \mathbb{Z}\} \\ &= \{(2a - b) + (a + 2b)\sqrt{-1} : a, b \in \mathbb{Z}\}.\end{aligned}$$

One can show more generally that for any nonzero $\beta \in \mathbb{Z}[\sqrt{-1}]$, the principal ideal $(\beta) \leq \mathbb{Z}[\sqrt{-1}]$ is a square lattice consisting of integer translations of the square with vertices

$$\{0, \beta, \beta\sqrt{-1}, \beta(1 + \sqrt{-1})\}.$$

(Why do these four vertices form a square?)

For parts (c) and (d), consider any $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ with $\beta \neq 0$. We want to find $\mu, \rho \in \mathbb{Z}[\sqrt{-1}]$ such that

- $\alpha = \mu\beta + \rho$,
- $\rho = 0$ or $\sigma(\rho) < \sigma(\beta)$.

Choose $\mu \in \mathbb{Z}[\sqrt{-1}]$ such that $|\alpha - \mu\beta|$ is a minimum (this μ might not be unique) and let $\rho := \alpha - \mu\beta$. We want to show that $\rho = 0$ or $\sigma(\rho) < \sigma(\beta)$. Since $\beta \neq 0$, we know that (β) is a square lattice so that the α lies inside or on the boundary of some square. The worst case scenario is when α is at the exact center of a square (which may or may not be an element of $\mathbb{Z}[\sqrt{-1}]$, depending on what β is). Since each square has side length $|\beta|$ this implies that

$$|\rho| = |\alpha - \mu\beta| \leq \frac{\sqrt{2}|\beta|}{2} = \frac{1}{\sqrt{2}}|\beta|.$$

If $\rho = 0$ we are done, otherwise we have $1 \leq |\rho|$ and we can square both sides of the above inequality to get

$$\sigma(\rho) = |\rho|^2 \leq \frac{1}{2}|\beta|^2 < |\beta|^2 = \sigma(\beta),$$

as desired. □

[Consider the ring $\mathbb{Z}[\sqrt{-2}]$ with size function $\sigma(a + b\sqrt{-2}) := |a + b\sqrt{-2}|^2 = a^2 + 2b^2$. Each nonzero principal ideal (β) now looks like a lattice of **rectangles** of dimension $|\beta| \times \sqrt{2}|\beta|$. Given $\alpha \in \mathbb{Z}[\sqrt{-2}]$, choose $\mu \in \mathbb{Z}[\sqrt{-2}]$ such that $|\alpha - \mu\beta|$ is minimal. The worst case scenario is when α is at the exact center of a rectangle, in which case $|\alpha - \mu\beta| \leq \frac{\sqrt{3}}{2}|\beta|$. In other words, $\sigma(\alpha - \mu\beta) \leq \frac{3}{4}\sigma(\beta) < \sigma(\beta)$, which is good. However, if you try to extend this proof to $\mathbb{Z}[\sqrt{-3}]$, something bad happens because the center of a $1 \times \sqrt{3}$ rectangle is **exactly** 1 unit from each vertex, which is not close enough! Indeed, we will see in the next problem that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, so it can't be Euclidean.]

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).]

Proof. For part (a) let $\alpha = a + b\sqrt{-3}$ and $\beta = c + d\sqrt{-3}$, so that $\alpha\beta = (a + b\sqrt{-3})(c + d\sqrt{-3}) = (ac - 3bd) + (ad + bc)\sqrt{-3}$. Now observe that

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 + 3b^2)(c^2 + 3d^2) \\ &= a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2, \end{aligned}$$

and that

$$\begin{aligned}
N(\alpha\beta) &= (ac-3bd)^2 + 3(ad+bc)^2 \\
&= a^2c^2 - 6abcd + 9b^2d^2 + 3a^2d^2 + 6abcd + 3b^2d^2 \\
&= a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2 \\
&= N(\alpha)N(\beta).
\end{aligned}$$

Alternatively, you could just say that the absolute value of complex numbers is multiplicative, but **someone** needed to prove that once upon a time (it was Diophantus).

For part (b) assume that $\alpha \in \mathbb{Z}[\sqrt{-3}]$ is a unit, i.e., assume there exists $\beta \in \mathbb{Z}[\sqrt{-3}]$ such that $\alpha\beta = 1$. Then by part (a) we have

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1.$$

Since $N(\alpha), N(\beta)$ are nonnegative integers this implies that $N(\alpha) = N(\beta) = 1$. Conversely, consider $\alpha = a+b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ with $N(\alpha) = a^2+3b^2 = 1$. Note that the complex conjugate $\bar{\alpha} = a - b\sqrt{-3}$ is also in $\mathbb{Z}[\sqrt{-3}]$ and we have

$$\alpha\bar{\alpha} = |\alpha|^2 = N(\alpha) = 1.$$

It follows that α is a unit with inverse $\bar{\alpha}$.

For part (c), let $\alpha = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ be a unit so that $N(\alpha) = a^2 + 3b^2 = 1$ by part (b). If $b \neq 0$ then we have $b^2 \geq 1$ and hence

$$1 = a^2 + 3b^2 \geq a^2 + 3 \geq 3.$$

This contradiction shows that $b = 0$, and then $a^2 + 0 = 1$ implies that $a = \pm 1$. That is, the only possible units of $\mathbb{Z}[\sqrt{-3}]$ are ± 1. Since both of these **are** units, we conclude that $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$.

For part (d), suppose for contradiction that we have $N(a+b\sqrt{-3}) = a^2+3b^2 = 2$. If $b \neq 0$ then we have $b^2 \geq 1$ and hence

$$2 = a^2 + 3b^2 \geq a^2 + 3 \geq 3,$$

contradiction. Otherwise we have $b = 0$ and hence $a^2 = 2$. But this is impossible because $\sqrt{2}$ is not an integer. Thus there is no element of norm 2.

For part (e), consider $\alpha \in \mathbb{Z}[\sqrt{-3}]$ with $N(\alpha) = 4$ and assume for contradiction that α is **reducible**, so we have $\alpha = \beta\gamma$ where β and γ are not units. By part (a) we have $N(\alpha) = N(\beta)N(\gamma)$ and by part (b) we know that $N(\beta) \neq 1$ and $N(\gamma) \neq 1$. It follows that $N(\beta) = N(\gamma) = 2$, which is imossible by part (d).

For part (f), consider the factorizations $2 \cdot 2 = 4 = (1+\sqrt{-3})(1-\sqrt{3})$. Since

$$N(2) = N(1 \pm \sqrt{-3}) = 4,$$

we know from part (e) that 2 and $1 \pm \sqrt{-3}$ are irreducible. We also know from part (c) that the only associates of 2 are ± 2 and hence 2 is not associate to either of $1 \pm \sqrt{-3}$. We conclude that 4 has two **different** irreducible factorizations. Thus number theory is more difficult/interesting than one might expect. □

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 $\text{ev}_\alpha : K[x] \to L$ by

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

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

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

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

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

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 $K[\alpha] := \text{im}\,(\text{ev}_\alpha)$ 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.]

Proof. For part (a), first note that $\text{ev}_\alpha(1) = 1$. Then for any $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ in $K[x]$ note that

$$\begin{aligned}
\text{ev}_\alpha(f+g) &= \text{ev}_\alpha\left(\sum_k (a_k+b_k)x^k\right) \\
&= \sum_k (a_k+b_k)\alpha^k \\
&= \sum_k a_k\alpha^k + \sum_k b_k\alpha^k \\
&= \text{ev}_\alpha(f) + \text{ev}_\alpha(g)
\end{aligned}$$

and

$$\begin{aligned}
\text{ev}_\alpha(fg) &= \text{ev}_\alpha\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) \\
&= \sum_k \left(\sum_{i+j=k} a_i b_j\right) \alpha^k \\
&= \sum_k a_k\alpha^k \cdot \sum_k b_k\alpha^k \\
&= \text{ev}_\alpha(f)\cdot\text{ev}_\alpha(g).
\end{aligned}$$

[Notice that we needed the fact that K is commutative in the proof of $\text{ev}_\alpha(fg) = \text{ev}_\alpha(f)\text{ev}_\alpha(g)$. So be careful when evaluating polynomials over noncommutative rings.]

For part (b) we suppose that $m_\alpha(x) \neq 0$. (Do you want to call the zero polynomial irreducible? I don't. Sorry, I probably should have mentioned that in the problem.) Now assume for contradiction that $m_\alpha(x)$ is **reducible**, i.e., assume we have

$$m_\alpha(x) = f(x)g(x)$$

where $f, g \in K[x]$ have degrees strictly between 1 and $\deg(m_\alpha)$. Evaluating at α gives $0 = m_\alpha(\alpha) = f(\alpha)g(\alpha)$ and since K is a domain this implies that $f(\alpha) = 0$ or $g(\alpha) = 0$. Without loss of generality, suppose that $f(\alpha) = 0$, and hence $f \in \ker(\text{ev}_\alpha) = (m_\alpha)$. This implies that $m_\alpha(x)$ divides $f(x)$ and hence $\deg(m_\alpha) \leq \deg(f)$, which contradicts the fact that $\deg(f) < \deg(m_\alpha)$. We conclude that $m_\alpha(x)$ is irreducible.

For part (c) assume that $\text{ev}_\alpha : K[x] \to L$ is not injective, that is, assume that $\ker(\text{ev}_\alpha) = (m_\alpha(x)) \neq (0)$. To show that $(m_\alpha(x))$ is maximal we assume for contradiction that there exists an ideal $(m_\alpha(x)) < J < K[x]$. Since $K[x]$ is a PID we have $J = (g(x))$ for some

$g(x) \in K[x]$. But then $g(x)$ divides $m_\alpha(x)$ (because $(m_\alpha(x)) \leq (g(x))$); $g(x)$ is not associate to $m_\alpha(x)$ (because $(m_\alpha(x)) \neq (g(x))$); and $g(x)$ is not a unit (because $(g(x)) \neq K[x]$). Thus $g(x)$ is a **proper divisor** of $m_\alpha(x)$, which contradicts the fact that $m_\alpha(x)$ is irreducible. We conclude that $(m_\alpha(x)) < K[x]$ is a maximal ideal. Finally, the First Isomosphism Theorem and a result from class imply that

$$K[\alpha] = \mathrm{im}\,(\mathrm{ev}_\alpha) \approx K[x]/\ker(\mathrm{ev}_\alpha) = K[x]/(m_\alpha(x))$$

is a field. $\square$

[For example, $\mathbb{R}[i] = \mathbb{C}$ is a field, but you already knew that. More interestingly, $\mathbb{Q}[\sqrt[3]{2}]$ is a field. How do you compute inverses in this field?]

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 $\deg(fg) = \deg(f) + \deg(g)$.]

Proof. Assume for induction that a polynomial of degree n over a field has at most n roots in any field extension. Now let $L \supseteq K$ be a field extension and consider $f(x) \in K[x]$ of degree $n+1$. We will show that $f(x)$ has at most $n+1$ roots in L. If $f(x)$ has no roots in L we're done, so suppose that there exists $\alpha \in L$ such that $f(\alpha) = 0$. By Descartes' Factor Theorem we have

$$f(x) = (x - \alpha)g(x)$$

where $g(x) \in L[x]$. Since $n + 1 = \deg(f) = \deg(x - \alpha) + \deg(g) = 1 + \deg(g)$ we conclude that $\deg(g) = n$. Now let $\beta \in L$ be any **other** root of $f(x)$. That is, assume that $\beta \neq \alpha$ and $f(\beta) = 0$. Then we have

$$0 = f(\beta) = (\beta - \alpha)g(\beta).$$

Since $\beta - \alpha \neq 0$ this implies that $g(\beta) = 0$. But by induction $g(x)$ has at most n distinct roots in L. We conclude that $f(x)$ has at most $n+1$ roots in L. $\square$

[The most common application of this is the following: Let $f(x)$ be a polynomial and suppose that $f(x)$ has infinitely many roots. Then $f(x)$ is the zero polynomial. This result fails over noncommutative rings. For example, the polynomial $f(x) = x^2 \in \mathbb{R}[x]$ has infinitely many roots in the ring of 2×2 matrices:

$$\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ for all } \alpha \in \mathbb{R}.$$

Where did the proof go wrong?]