Math 562 Spring 2012
Homework 2 Drew Armstrong

Problems on General Rings

1. We say that a general ring R is (right) Artinian if every descending chain of (right) ideals terminates. That is, given ideals $R \supseteq I_1 \supseteq I_2 \supseteq \cdots$ there exists some $k \geq 1$ such that $I_k = I_{k+1} = \cdots$. **Prove** that $ab = 1$ implies $ba = 1$ in an Artinian ring. [Hint: Consider the descending chain of right ideals $R \supseteq bR \supseteq b^2R \supseteq \cdots$ (I don't use the notation (b^2) since R is not commutative). Show that there exists some $c \in R$ with $b^k = b^{k+1}c$.]

Proof. Suppose that $ab = 1$ in a (right) Artinian ring R and consider the descending chain of right ideals $R \supseteq bR \supseteq b^2R \supseteq \cdots$. Since R is Artinian there must exist k such that $b^kR = b^{k+1}R$. Then since $b^k \in b^kR = b^{k+1}R$ there must exist $c \in R$ such that $b^k = b^{k+1}c$. Now multiply on the left by a^k to obtain $1 = a^kb^k = a^kb^{k+1}c = bc$. Finally, note that

$$a = a1 = a(bc) = (ab)c = 1c = c.$$

We conclude that $1 = bc = ba$. □

Problems on Integral Domains

2. Let R be an integral domain. We say that $a, b \in R$ are associates if $b = ua$ where u is a unit. **Prove** that a and b are associates if and only if $(a) = (b)$.

Proof. We may assume that $ab \neq 0$ otherwise there is nothing to do.

So suppose that $a = ub$, where u is a unit. Since a is a multiple of b we have $a \in (b)$, from which it follows that $(a) \subseteq (b)$. Similarly, since $b = u^{-1}a$ we conclude that $(b) \subseteq (a)$. Hence $(a) = (b)$.

Conersely, suppose that $(a) = (b)$. Since $a \in (b)$ and $b \in (a)$ we have $a = ub$ and $b = va$ for some $u, v \in R$. Combining the two equations gives $a = ub = uva$, and then $a(1 - uv) = 0$. Finally, using the fact that R is an integral domain we get $1 = uv$. Hence a, b are associates. □

3. We say that a is a proper divisor of b if $b = aq$ and neither a nor q is a unit. **Prove** that a is a proper divisor of b if and only if $(b) < (a) < (1)$ — where " $<$ " means strict containment of ideals.

Proof. Note that a is a divisor of b if and only if $(b) \subseteq (a) \subseteq (1)$. By Problem 2.2 the first inequality is strict if and only if a is **not** associate to b. By Problems 2.2 and 1.2 (from the first homework), the second inequality is strict if and only if a is **not** a unit. Hence a is a **proper** divisor of b if and only if $(b) < (a) < (1)$; i.e. both inequalities are strict. □

It's good to have alternate definitions for important concepts. The next two problems show that "integral domain" equals "subring of a field".

4. Let R be a subring of a field (i.e. suppose there exists a field $\mathbb{F}$ and an injective homomorphism $\iota : R \to \mathbb{F}$). **Prove** that R is an integral domain.

Proof. Let $a, b \in R$ and suppose that $ab = 0$. Now map this equation into the field to get $\iota(a)\iota(b) = \iota(0) = 0$. If $\iota(a) = 0$ then by injectivity we have $a = 0$, and we are done. Otherwise, since $\mathbb{F}$ is a field, we may divide by $\iota(a)$ to get $\iota(b) = \iota(a)^{-1} \cdot 0 = 0$. Then injectivity implies $b = 0$. □

5. Let R be an integral domain. Put an equivalence relation on the set R^2 of ordered pairs by saying $(a, b) \sim (c, d)$ if and only if $ad = bc$, and let $[(a, b)]$ denote the $\sim$-class of (a, b). Now define the field of fractions of R,

$$\text{Frac}(R) := \{[(a, b)] : b \neq 0\},$$

with product $[(a, b)] \times [(c, d)] := [(ac, bd)]$ and sum $[(a, b)] + [(c, d)] := [(ad + bc, bd)]$.

(a) Show that $\times$ and $+$ are well-defined on equivalence classes. (It follows that Frac(R) is a field, but you don't need to verify the boring details.)

(b) Show that the map $\iota(a) := [(a, 1)]$ is an injective homomorphism $\iota : R \to \text{Frac}(R)$.

[Hint: A better name for $[(a, b)]$ might be a/b. Look in the book.]

Proof. To prove (a), suppose that $[(a, b)] = [(A, B)]$ (i.e. $aB = Ab$) and $[(c, d)] = [(C, D)]$ (i.e. $cD = Cd$). Note that multiplication is well-defined, i.e.

$$[(a, b)] \times [(c, d)] = [(ac, bd)] = [(AC, BD)] = [(A, B)] \times [(C, D)],$$

because $(ac)(BD) = (aB)(cD) = (Ab)(Cd) = (AC)(bd)$. Note that addition is well-defined, i.e.

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] = [(AD + BC, BD)] = [(A, B)] + [(C, D)],$$

because

$$\begin{aligned}(ad + bc)(BD) &= (ad)(BD) + (bc)(BD) \\ &= (aB)(dD) + (bB)(cD) \\ &= (Ab)(dD) + (bB)(Cd) \\ &= (AD)(bd) + (BC)(bd) \\ &= (AD + BC)(bd).\end{aligned}$$

To prove (b) we first show that ι is a homomorphism. Given $a, b \in R$ we have

$$\iota(a) + \iota(b) = [(a, 1)] + [(b, 1)] = [(a + b, 1)] = \iota(a + b)$$

and

$$\iota(a) \times \iota(b) = [(a, 1)] \times [(b, 1)] = [(ab, 1)] = \iota(ab).$$

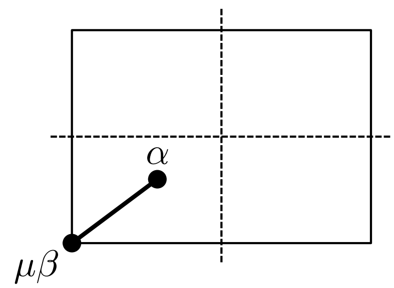
Note that $[(1, 1)]$ is the multiplicative identity for $\mathbb{F}$ and $\iota(1) = [(1, 1)]$, as desired. Finally, we need to show that ι is injective. So suppose that $\iota(a) = [(a, 1)] = [(b, 1)] = \iota(b)$. This implies that $(a, 1) \sim (b, 1)$, or $a = a1 = 1b = b$. $\square$

Problems on Subrings of $\mathbb{C}$

6. Show that the subring $\mathbb{Z}[\sqrt{-2}] := \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ with the norm function $N(a + b\sqrt{-2}) := a^2 + 2b^2$ is a Euclidean domain. [Hint: The principal ideal $(0) \neq (\beta) \subseteq \mathbb{Z}[\sqrt{-2}]$ is a grid of rectangles with side lengths $|\beta|$ and $\sqrt{2}\,|\beta|$. Recall the proof for $\mathbb{Z}[\sqrt{-1}]$.]

Proof. Given nonzero $\beta \in \mathbb{Z}[\sqrt{-2}]$, note that the principal ideal (β) is a grid of rectangles with side lengths $|\beta|$ and $\sqrt{2}\,|\beta|$. To see this, note that (β) is just β applied to every element of the lattice $(1) = \mathbb{Z}[\sqrt{-2}]$. Multiplication by the complex number β is geometrically a rotation (by some angle) combined with a dilation by $|\beta|$.

To divide $\alpha \in \mathbb{Z}[\sqrt{-2}]$ by β we will consider α relative to the principal ideal $(\beta) \neq (0)$, and choose $\mu \in \mathbb{Z}[\sqrt{-2}]$ such that $|\alpha - \mu\beta|$ is minimal (i.e. $\mu\beta$ is an element of the lattice (β) that is closest to α; possbly not unique). Note that α will occur inside or on the boundary of some $|\beta|$ by $\sqrt{2}\,|\beta|$ rectangle.



Note that the distance $|\alpha - \mu\beta|$ is less than or equal to half of the diagonal of the rectangle, i.e. $|\alpha - \mu\beta| \le (\sqrt{3}/2)\,|\beta| < |\beta|$. Using the norm function $N(a + b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = a^2 + 2b^2$, we can rephrase this as $N(\alpha - \mu\beta) < N(\beta)$.

In summary: Given $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$, there exist μ and $\rho = \alpha - \mu\beta$ such that

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

We conclude that $\mathbb{Z}[\sqrt{-2}]$ with norm function N is a Euclidean domain. $\square$

7. Consider the subring $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{C}$ with norm $N(a + b\sqrt{-3}) := a^2 + 3b^2$.

(a) Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[\sqrt{-3}]$.
(b) Show that $u \in \mathbb{Z}[\sqrt{-3}]$ is a unit if and only if $N(u) = 1$.
(c) Show that $N(\alpha) = 4$ implies that $\alpha \in \mathbb{Z}[\sqrt{-3}]$ is irreducible.
(d) Show that $4 \in \mathbb{Z}[\sqrt{-3}]$ can be factored into irreducibles in **two distinct ways**.

Proof. To show (a), note that $N(a + b\sqrt{-3}) = |a + b\sqrt{-3}|^2 = |a + ib\sqrt{3}|^2 = a^2 + 3b^2$. Thus we can obtain the multiplicativity of N from the multiplicativity of absolute value on $\mathbb{C}$:

$$N(\alpha\beta) = |\alpha\beta|^2 = (|\alpha|\,|\beta|)^2 = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta).$$

To show (b), suppose that $u \in \mathbb{Z}[\sqrt{-3}]$ is a unit; i.e. suppose that there exists $v \in \mathbb{Z}[\sqrt{-3}]$ with $uv = 1$. Applying N gives $N(u)N(v) = N(1) = 1$. Then since $N(u), N(v)$ are positive integers we get $N(u) = 1$. Conversely, suppose that $u = a + b\sqrt{-3}$ satisfies $N(u) = a^2 + 3b^2 = 1$. This implies that $(a, b) = (1, 0)$ (i.e. $u = 1$) or $(a, b) = (-1, 0)$ (i.e. $u = -1$). In either case u is a unit. As a corollary of this proof, we have also shown that $\mathbb{Z}[\sqrt{-3}]^\times = \{\pm 1\}$.

To show (c), suppose for contradiction that $N(\alpha) = 4$ and that α has a **nontrivial** factorization $\alpha = \beta\gamma$. Since $N(\beta)N(\gamma) = N(\alpha) = 4$ and since β, γ are not units, we conclude from part (b) that $N(\beta) = N(\gamma) = 2$. However, $\mathbb{Z}[\sqrt{-3}]$ contains no element of norm 2 because the equation $a^2 + 3b^2 = 2$ has no integer solution. Contradiction.

To show (d), first note that

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

Since 2, $1 + \sqrt{-3}$, and $1 - \sqrt{-3}$ all have norm 4, they are irreducible by part (c). Then since the units of $\mathbb{Z}[\sqrt{-3}]$ are $\{\pm 1\}$ we observe that 2 is not associate to either of $1 \pm \sqrt{-3}$. Thus we have obtained two distinct irreducible factorizations of 4. $\square$

We conclude that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD, hence it's not a PID, hence it's not Euclidean. If you try to prove that $\mathbb{Z}[\sqrt{-3}]$ is Euclidean using the argument from Problem 5, you will see that the center point of a $|\beta| \times \sqrt{3}\,|\beta|$ rectangle is **exactly** $|\beta|$ away from the closest vertex. That's too far away.