MAT1100

Algebra I

Assignment 4

Contents

Tyler Holden - Fall 2011

1. Problem 1

Clearly all principal ideal domains are unique factorization domains. Hence all the remains to be shown is that unique factorization domains in which $\gcd(a, b) \in (a, b)$ are actually principal ideal domains.

Lemma 1.1. *If R is a unique factorization domain in which $\gcd(a, b) \in (a, b)$ then $(\gcd(a, b)) = (a, b)$.*

Proof. Let $q = \gcd(a, b)$ so that $q \in (a, b)$. This means that $\exists s, t \in R$ such that $q = as + bt$. Now if $p \in (\gcd(a, b))$ then $p = qr$ for some $r \in R$, and so

$$p = qr = a(sr) + b(tr) \in (a, b)$$

which tells us that $(\gcd(a, b)) \subseteq (a, b)$.

Conversely, we know that $q|a$ and $q|b$ so that $a \in (q)$ and $b \in (q)$. Let $c \in (a, b)$ and write $c = as + bt$ and note that $a \in (q)$ implies $as \in (q)$ and similarly $bt \in (q)$. Hence $as + bt \in (q)$ and so we conclude that $(a, b) \subseteq (\gcd(a, b))$.

Both inclusions gives the desired result. □

Let $I \subseteq R$ be a finitely generated ideal, say $I = (n_1, \ldots, n_k)$. Since $(n_1, n_2) = (\gcd(n_1, n_2))$ we can rewrite $I = (\gcd(n_1, n_2), n_3, \ldots, n_k)$. Continuing recursively, we find that

$$I = (\gcd(n_k, \gcd(n_{k-1}, \gcd(n_{k-2}, \ldots))))$$

which is principal.

Now all that remains is to show that this exhausts all possible ideals. In particular, there are no infinitely generated ideals. Before we can do this, we will need the following two lemmas.

Lemma 1.2. *If R is a unique factorization domain, then R satisfies the ascending chain condition on principal ideals. That is, if*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq$$

is an strictly increasing chain of principal ideals, then this chain eventually stabilizes.

Proof. Assume that we are given an ascending chain of principal ideals of the form

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq .$$

We recall that if we write a_1 and a_2 as a product of primes, then every prime factor of a_2 is in a_1. Since in particular our chain is increasing, this means that the set of prime factors of a_2 is strictly less than a_1. Since a_1 is a finite product of primes and at each stage of chain we reduce the number of prime-factors, the chain must eventually stabilize. □

This next lemma will tell us there are no infinitely generated ideals which will conclude the proof, since we have shown that all finitely generated ideals are principal.

Lemma 1.3. *If R is a unique factorization domain such that* $\gcd(a,b) \in (a,b)$ *then there are no infinitely generated ideals.*

Proof. For the sake of contradiction, assume that there is an infinitely generated ideal, say $I \subseteq R$. We will construct a non-stabilizing ascending chain of principal ideals which will contradict Lemma 1.2.

Construct the chain as follows. Since I is infinitely generated, it is non-empty. Choose $c_1 = b_1 \in I$ and note that $I \setminus (b_1) \neq \emptyset$ since otherwise I would be finitely generated. Choose $b_2 \in I \setminus (b_1)$ and define $c_2 = \gcd(b_1, b_2)$. By Lemma 1.1, we have that $(c_2) = (b_1, b_2)$ and so clearly

$$(c_1) \subsetneq (c_2)$$

where the inclusion is strict by our choice of b_2.

Assume then that we have selected a series of elements $\{c_1, \ldots, c_{k-1}\}$ in I such that

$$(c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_{k-1}).$$

It must follow that $I \setminus (c_1, c_2, \ldots, c_{k-1}) \neq \emptyset$ since the I would be finitely generated. Take $b_k \in I \setminus (c_1, c_2, \ldots, c_{k-1})$ and set $c_k = \gcd(c_{k-1}, b_k)$. By Lemma 1.1 we have $(c_k) = (c_{k-1}, b_k)$ so $(c_{k-1}) \subseteq (c_k)$ and our chain now looks like

$$(c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_{k-1}) \subsetneq (c_k).$$

Now this process will never terminate since I is infinitely generated. But this contradicts the ascending chain condition on principal ideals, so we conclude there are no infinitely generated ideals. □

2. Problem 2

2.1. **Part a.** Assume that R is commutive. Our first order of business will be to show that $\eta(R)$ is a subgroup of R. Let $x, y \in \eta(R) \setminus 0$ with $n, m \in \mathbb{N}$ minimal such that $x^n = y^m = 0$. Note that $n, m \geq 2$ since $x, y \neq 0$. Now R is commutative so we can apply the binomial theorem to find that

$$(x+y)^{nm+1} = \sum_{k=0}^{nm+1} \binom{nm+1}{k} x^k y^{mn+1-k}.$$

In this summation, if $k > n$ then $x^k = 0$ so all such terms disappear. On the other hand, if $k \leq n$ then

$$nm + 1 - k \geq mn + 1 - n = n(m-1) + 1 > m$$

and so $y^{nm+1-k} = 0$. Both cases imply that $(x+y)^{nm+1} = 0$ so that $x + y \in \eta(R)$ and $\eta(R)$ is closed under addition. Now $0 \in \eta(R)$ since $0^1 = 0$. Associativity and the fact that 0 acts as identity are inherited from the underlying group of the ring. All that remains to be shown is the presence of the inverse. Assume that $x \in \eta(R)$ with $x^n = 0$. Then $(-x)^n = (-1)^n x^n = 0$ so $-x \in \eta(R)$ and we conclude that $\eta(R)$ is a group as required.

To show that $\eta(R)$ is an ideal, let $x \in \eta(R)$ and $r \in R$ be arbitrary. Then $(rx)^n = r^n x^n = 0$ by commutativity, so $rx \in \eta(R)$ and we conclude that $\eta(R)$ is an ideal as required.

2.2. **Part b.** Consider the ring $M_2(\mathbb{R})$ of 2×2 matrices with real coefficients. Now

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

so $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \eta(M_2(\mathbb{R}))$. On the other had,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

which one can easily see is idempotent and so satisfies

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & n \text{ even} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & n \text{ odd} \end{cases}$$

and so is never zero. This implies that $\eta(M_2(\mathbb{R}))$ is not a subgroup of the underling abelian group of R and hence cannot be an ideal.

3. Problem 3

In order to show the desired result, consider the following lemma:

Lemma 3.1. *The sum of a nilpotent element with a unit is a unit.*

Proof. Let u be a unit and x a nilpotent with $n \in \mathbb{N}$ minimal such that $x^n = 0$. We notice first that $1 + x$ is a unit. Indeed

$$\begin{aligned} (1-x)(1 + x + x^2 + \cdots + x^n) &= (1 + x + \cdots + x^n) - (x + \cdots + x^{n+1}) \\ &= 1 - (-1)^n x^{n+1} \\ &= 1 \end{aligned}$$

since $x^{n+1} = 0$ by assumption. Now notice that $u^{-1}x$ is nilpotent since $(u^{-1}x)^n = u^{-n}x^n = 0$, so $1 + u^{-1}x$ is a unit, and since the units of a ring form a multiplicative group,

$$u(1 + u^{-1}x) = u + x$$

is also a unit, which is precisely what we wanted to show. □

Assume then that $p(x) = \sum_{k=0}^{n} a_k x^k \in A[x]$ such that a_0 is a unit and a_i is nilpotent for each $i = 1, \ldots, n$. Now $a_i x^i$ is nilpotent since if $a_i^n = 0$ then $(a_i x^i)^n = a_i^n x^{in} = 0$. It is then clear that a_0 is a unit by assumption, so $a_0 + a_1 x$ is a unit since $a_1 x$ is nilpotent. Inductively, we see that $a_0 + a_1 x + \cdots + a_n c^n$ is a unit, which is precisely what we wanted to show.

Conversely, assume that $p(x) = \sum_{k=0}^{n} a_k x^k$ is a unit. We will proceed by induction on the order of $\deg p(x)$.

Base Case:

For $\deg p(x) = 1$ we have that $p(x) = a_0$. If $q(x)$ is such that $p(x)q(x) = 1$ then $q(x) = b_0$ for some b_0 since higher order terms would not disappear. Thus a_0 is a unit, and all other terms are vacuously nilpotent (since there are no other terms).

Induction Hypothesis:

Assume that if $\deg p(x) = n - 1$ is a unit, then a_0 is a unit and a_i is nilpotent for all $i = 1, \ldots, n-1$.

Induction Step:

Let $p(x) = \sum_{k=0}^{n} a_k x^k$ be a unit with inverse $q(x) = \sum_{\ell=0}^{m} b_\ell x^\ell$. Then

$$1 = p(x)q(x) = \sum_{i=0}^{m+n} \left(\sum_{j=0}^{k} a_j b_{k-j} \right).$$

By looking at the constant term corresponding to $k = 0$, we see that $a_0 b_0 = 1$ and so a_0 is a unit. By examining the $(n+m)^{th}$ term we see that $a_n b_m = 0$. Similarly, the $(n+m-1)^{th}$ term tells us that $a_{n-1} b_m + a_n b_{m-1} = 0$. Multiplying by a_n we get

$$a_{n-1}\cancelto{0}{(a_n b_m)} + a_n^2 b_{m-1} = a_n^2 b_{m-1} = 0.$$

We claim that $a_n^{k+1} b_{m-k} = 0$. Indeed, via the principal of strong induction, asume that $a_n^{i+1} b_{m-i} = 0$ for all $i = 1, \ldots, k-1$. Now $\sum_{j=0}^{k} a_j b_{k-j} = 0$ and so mutliplying by a_n^k we find

$$\begin{aligned} 0 = a_n^k \sum_{j=0}^{k} a_j b_{k-j} &= \sum_{j=0}^{k} a_n^k a_j b_{k-j} \\ &= a_n^{k+1} b_k \end{aligned}$$

and hence our result holds true. Continuing this process, we eventually see that $a_n^m b_0 = 0$. Since $a_0 b_0 = 1$ we can multiply by a_0 to get

$$a_0(a_n^m b_0) = a_n^m (a_0 b_0) = a_n^m = 0$$

so a_n is nilpotent.

Now define $r(x) = p(x) - a_n x^n$. Since $r(x)$ is the sum of a unit and a nilpotent element Lemma 3.1 tells us that $r(x)$ is a unit whose $n-1$ terms agree with $p(x)$. Furthermore, $\deg r(x) = n-1$ and so by the induction hypothesis, all other terms of $p(x)$ other than a_0 are nilpotent, which is precisely what we wanted to show.

4. Problem 4

Since all Euclidean domains are Principal Ideal Domains are Unique Factorization Domains, it is sufficient to show that $\mathbb{Z}[i]$ is a Euclidean domain. Define $N : \mathbb{Z}[i] \to \mathbb{N}$ by $N(a+ib) = a^2 + b^2$. We claim that this is a Euclidean valuation. First note that N is multiplicative since if $a+bi, c+di \in \mathbb{Z}[i]$ then

$$\begin{aligned} N\Big((a+bi)(c+di)\Big) &= N\Big((ac-bd) + i(bc+ad)\Big) \\ &= (ac-bd)^2 + (bc+ad)^2 \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2. \end{aligned}$$

On the other hand

$$N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2) \qquad = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$

so $N(\alpha\beta) = N(\alpha)N(\beta)$. Thus we note that if $\alpha, \beta \neq 0$ then $N(\alpha\beta) \leq N(\alpha)$ and $N(\alpha\beta) \leq N(\beta)$ as required.

Now let $\alpha, \beta \in \mathbb{Z}[i]$. We notice that $\mathbb{Z}[i]$ is a lattice in $\mathbb{C}[i]$ and that (b) is a sublattice of that lattice. In particular, a must lie in one of "boxes" of this sublattice. Our goal will be to choose the closest point to a of this sublatice, whose error will give us the desired remainder. Let $\alpha = a+ib$ and $\beta = c+di$ and notice that

$$\begin{aligned} \frac{\alpha}{\beta} = \frac{a+ib}{c+id} &= \frac{a+ib}{c+id}\frac{c-id}{c-id} \\ &= \frac{(ac-bd) + i(bc+ad)}{c^2+d^2}. \end{aligned}$$

Now choose the closest rational number n to $\frac{ac-bd}{c^2+d^2}$ and m to $\frac{bc+ad}{c^2+d^2}$ so that

$$\left|\frac{ac-bd}{c^2+d^2} - n\right|, \left|\frac{bc+ad}{c^2+d^2} - m\right| \leq \frac{1}{2}.$$

Define $q = (n+im)$ and $r = \alpha - \beta q$. We claim that $N(r) < N(\beta)$.

Indeed, define the "error" in our approximation by

$$\epsilon = \left(\frac{ac-bd}{c^2+d^2} - n\right) + i\left(\frac{bc+ad}{c^2+d^2} - m\right)$$

and notice then that $r = \beta\epsilon$. Now

$$N(\epsilon) = \left|\frac{ac-bd}{c^2+d^2} - n\right| + \left|\frac{bc+ad}{c^2+d^2} - m\right| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

and so

$$N(r) = N(\beta\epsilon) = N(\beta)N(\epsilon) < \frac{1}{2}N(\beta) < N(\beta)$$

which is precisely what we wanted to show.

If u is a unit in $\mathbb{Z}[i]$ such that $uv = 1$ then we find that $N(uv) = N(u)N(v) = N(1) = 1$ so that $N(u)$ and $N(v)$ are units $\mathbb{N}$. However, the only unit in $\mathbb{N}$ is 1 which implies that $N(u) = N(v) = 1$. If $a + bi$ is a unit in $\mathbb{Z}[i]$ then we must have that $a^2 + b^2 = 1$ which is only possible if $a = \pm 1$ or $b = \pm 1$ exclusively. This corresponds to ± 1 and $\pm i$ and so this is the complete set of units in $\mathbb{Z}[i]$.

5. Problem 5

To find the greatest common divisor of 85 and $1 + 13i$ we apply the Euclidean algorithm. Indeed, note that

$$\begin{aligned} 85 &= (1 - 7i)(1 + 13i) + (-7 - 6i) \\ 1 + 13i &= (-7 - 6i) * (-1 - i) + 0 \end{aligned}$$

so $(-7 - 6i)$ is the greatest common divisor of 85. We note that this is only the gcd up to association, so the complete set of gcd's is given by

$$7 + 6i, \quad -7 - 6i, \quad 6 - 7i, \quad -6 + 7i.$$

To express this as a linear combination, we work through the Euclidean algorithm in reverse. However, this is trivial since we attain the gcd after a single application, so

$$-7 - 6i = (1)85 + (-1 + 7i)(1 + 13i).$$

6. Problem 6

Let $R = \mathbb{Q}[x, y]/(x^2 + y^2 - 1)$ which we want to show is not a unique factorization domain. Let square brackets [] denote equivalence classes in R and notice that $[x^2 + y^2 - 1] = [0]$ in R so $[y^2] = [1 - x^2]$. In particular, if $p(x, y) \in \mathbb{Q}[x, y]$ then we can simply replace every instance of y^n as follows:

$$y^n = \begin{cases} (1 - x)^{\frac{n}{2}} & n \text{ even} \\ y(1 - x)^{\frac{n-1}{2}} & n \text{ odd} \end{cases}$$

and so every element of R can be written as $[p(x) + yq(x)]$ for $p(x), q(x) \in \mathbb{Q}[x]$. Define the function

$$\varphi : R \to R, \qquad [f(x, y)] \mapsto [f(x, -y)].$$

We claim that φ is an ring automorphism of R. Indeed, clearly $\varphi([1]) = [1]$ and

$$\begin{aligned} \varphi([f(x,y)][g(x,y)]) &= [f(x,-y)][g(x,-y)] \\ &= \varphi([f(x,y)])\varphi([g(x,y)]) \\ \varphi([f(x,y)+g(x,y)]) &= [f(x,-y)+g(x,-y)] = [f(x,-y)]+[g(x,-y)] \\ &= \varphi([f(x,y)])+\varphi([g(x,y)]) \end{aligned}$$

so ϕ is a ring homomorphism. But it is easily seen that $\phi \circ \phi = \text{id}$ so ϕ is bijective, and hence a ring automorphism.

Now define a psuedo-norm on R as function $N : R \to \mathbb{Q}[x]$ by $N([f]) = [f]\phi([f])$. Let $\alpha = [a(x) + yb(x)]$ and notice that

$$\begin{aligned} N(\alpha) &= [a(x)+yb(x)]\phi([a(x)+yb(x)]) \\ &= [a(x)+yb(x)][a(x)-yb(x)] \\ &= [a(x)^2 - y^2 b(x)] \\ &= [a(x)^2 - (1-x^2)b(x)] \end{aligned}$$

as identified with an element of $\mathbb{Q}[x]$. We claim that this function is multiplicative. Let $\beta = [c(x)+yd(x)]$, and for brevity of notation we will write $\alpha = [a(x)+yb(x)]$ as $\alpha = [a+yb]$; similarly, $\beta = [c + yd]$. Then computing yields

$$\begin{aligned} N\Big([a+yb][c+yd]\Big) &= N\Big((ac+(1-x^2)bd)+y(bc+ad)\Big) \\ &= (ac+(1-x^2)bd)^2 - (1-x^2)(bc+ad)^2 \\ &= a^2c^2 + (1-x^2)^2b^2d^2 - (1-x)^2b^2c^2 - (1-x^2)a^2d^2. \end{aligned}$$

On the other hand, we have that

$$\begin{aligned} N([a+yb])N([c+yd]) &= (a^2-(1-x^2)b^2)(c^2-(1-x^2)d^2) \\ &= a^2c^2 + (1-x^2)^2b^2d^2 - (1-x)^2b^2c^2 - (1-x^2)a^2d^2 \end{aligned}$$

and we conclude that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Consider the equivalence class $[x]$ which we claim is irreducible. Indeed, let $[f], [g] \in R$ be such that $[x] = [f][g]$. By multiplicativity of the norm, we then have that

$$N([x]) = N([f][g]) = N([f])N([g]).$$

However, we can easily calculate $N([x]) = x^2$ so that $N([f])N([g]) = x^2$. There are two possible cases:

Case 1:

Assume that $N([f]) = N([g]) = x$. Write $f = a+yb$ and note that $N(f) = a^2+(1-x^2)b^2$. Now for $N(f) = x$ we must have that $b = 0$ since otherwise $\deg N(f) \geq 2$ which cannot happen. Thus we have that $N(f) = a^2 = x$ which is impossible in $\mathbb{Q}[x]$ since no polynomial in $\mathbb{Q}[x]$ squares to x.

Case 2:

Assume that $N([g]) = x^2$ and $N([f]) = 1$. Again, take $f = a + yb$ so that $N([f]) = a^2 + (1-x^2)b^2 = 1$. We can again determine that $b = 0$ otherwise $\deg N([f]) \geq 2$ and so we are left with $a^2 = 1$ as a polynomial. Hence $[f] = a$ and satisfies $[f][f] = [a^2] = [1]$ so $[f]$ is a unit and $[x]$ is irreducible in R.

We are just about ready to show that R is not a unique factorization domain. Before we can do this however, we need the following Lemma

Lemma 6.1. *If $a, b \in S$ a ring, then*

$$\frac{R/(a)}{([b])} \cong R/(a,b).$$

Proof. It is sufficient to show that $([b]) = \frac{(a,b)}{(a)}$ since then the third isomorphism theorem tells us that

$$\frac{R/(a)}{([b])} \cong \frac{R/(a)}{(a,b)/(a)} \cong R/(a,b).$$

But this is easy to see, since

$$\begin{aligned} ([b]) &= \{[x][b] : [x] \in R/(a)\} \\ &= \{xb + (a) : x, b \in R\} \\ &\subseteq \frac{(a,b)}{(a)} \end{aligned}$$

On the other hand, let $x \in \frac{(a,b)}{(a)}$ and write this as $x = as + bt + (a)$ and notice that since (a) an ideal then $as \in (a)$ and so $x = bt + (a) \in ([b])$ so $\frac{(a,b)}{(a)} \subseteq (a,b)$. Both inclusions give the desired result. □

Now for the sake of contradiction, assume that $R = \mathbb{Q}[x,y]/(x^2+y^2-1)$ is a unique factorization domain. Since elements of UFDs are prime if and only if they are irreducible, then since we showed $[x]$ is irreducible, it must also be a prime. Hence we know that

$$\frac{\mathbb{Q}[x,y]/(x^2+y^2-1)}{([x])}$$

is an integral domain.

However, we can explicitly calculate this space using Lemma 6.1 to be

$$\begin{aligned} \frac{\mathbb{Q}[x,y]/(x^2+y^2-1)}{([x])} &\cong \frac{\mathbb{Q}[x,y]}{(x^2+y^2-1, x)} \\ &\cong \frac{\mathbb{Q}[x,y]/(x)}{([x^2+y^2-1])} \end{aligned}$$

Now we must figure out what $[x^2+y^2-1]$ looks like in $\mathbb{Q}[x,y]/(x)$. We can write this as $x^2+y^2-1+(x)$ and notice that $x^2 \in (x)$ so that $x^2+y^2-1+(x) = y^2-1+(x) = [y^2-1]$.

Furthermore, it is well known that $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$ and so we find

$$\begin{aligned}\frac{\mathbb{Q}[x,y]/(x^2+y^2-1)}{([x])} &\cong \frac{\mathbb{Q}[x,y]/(x)}{([x^2+y^2-1])} \\ &\cong \frac{\mathbb{Q}[y]}{y^2-1}\end{aligned}$$

But $\mathbb{Q}[y]/(y^2-1)$ is not an integral domain. Indeed, neither $[y+1]$ nor $[y-1]$ are zero but $[y+1][y-1] = [y^2-1] = [0]$ and so $\mathbb{Q}[y]/(y^2-1)$ contains zero divisors. This is a contradiction, and so $[x]$ cannot be prime.

Since $[x]$ is irreducible but not prime, we conclude that R is not a unique factorization domain.