Algebra I - MAT1100
Assignment # 4
Due: 29 November 2011
Jerrod Smith, student ID 998 689 138

Notation. For a ring R and a subset A of R, we denote by (A) the ideal generated by A.

1. Prove that a ring R is a PID if and only if it is a UFD in which $\gcd(a, b) \in (a, b)$ for every non-zero $a, b \in R$.

   Solution.

   Suppose that R is a PID. In particular R is a UFD. Let $a, b \in R \setminus \{0\}$ and consider the ideal (a, b). By assumption there exists $c \in R \setminus \{0\}$ such that $(c) = (a, b)$. Then since we have that $c \in (a, b)$ there exist $s, t \in R$ such that $c = as + tb$. Moreover, since $a, b \in (a, b) = (c)$ we have that $c|a$ and $c|b$. We claim that $c = \gcd(a, b)$. Suppose that $q|a$, $q|b$ then there exist $x, y \in R$ such that $a = xq$ and $b = yq$. Then

$$c = sa + tb = sxq + tyb = (sx + tb)q$$

   which implies that $c|q$ and c is the gcd of a and b. Therefore, in particular we have that $\gcd(a, b) \in (a, b)$.

   Conversely, suppose that R is a UFD such that $\gcd(a, b) \in (a, b)$ for every non-zero $a, b \in R$. We show that every ideal of R is principal. First, $\{0\} = (0)$ and $R = (1)$ are principal, if we consider R as an ideal (depends on convention). Our argument will proceed as follows:

   (i) UFDs satisfy the ascending chain condition for principal ideals (ACCP),

   (ii) under our assumption every finitely generated ideal is principal.

   (iii) in a UFD satisfying our hypothesis every ideal is finitely generated.

   First, suppose that

$$(a_1) \subsetneq (a_2) \subsetneq \dots$$

   is an infinite ascending chain of principal ideals in a UFD R. Then we have that $a_1 \in (a_2)$ and so $a_2|a_1$. Therefore any prime appearing in the factorization of a_2 appears in the factorization of a_1. Since the inclusion on ideals is strict we have that a_2 has strictly fewer prime factors. Similarly, $a_k \in (a_{k+1})$ for all k, and a_{k+1} must have strictly fewer prime factors than a_k. Since a_1 is a product of finitely many primes to finite powers, the chain of ideals must stabilize. This is a contradiction. Therefore, no such infinite chain if principal ideas of R exists and any UFD satisfies ACCP.

   Suppose that R is a UFD such that $\gcd(a, b) \in (a, b)$ for every non-zero $a, b \in R$. We show that every finitely generated ideal of R is principal. Let $I = (a_1, \dots, a_n)$ be a finitely generated ideal of R were $a_j \in R \setminus \{0\}$ for all j. Consider the ideal (a_1, a_2), by hypothesis $q_1 = \gcd(a_1, a_2) \in (a_1, a_2)$. In particular, $(q_1) \subset (a_1, a_2)$; moreover since $a_1 = p_1q_1$ and $a_2 = p_2q_1$ for some $p_1, p_2 \in R$ we have that for all $x, y \in R$

$$xa_1 + ya_2 = xp_1q_1 + yp_2q_1 = (xp_1 + yp_2)q_1 \in (q_1)$$

and so $(a_1, a_2) \subset (q_1)$. Therefore, $(a_1, a_2) = (q_1)$. We have $a_1, a_2 \in I$ and so $(a_1, a_2) \subset I$. Therefore we have $q_1 \in I$ and in particular we have that $I = (q_1, a_3, \ldots, a_n)$. By induction, we have that I is a principal ideal.

Finally, we show that every ideal of R is finitely generated. Suppose that J is an ideal of R that is not finitely generated. Write $J = (a_1, a_2, \ldots)$. If we have that $(a_1) = (a_1, a_2)$ we have $a_2 \in (a_1)$ and so $J = (a_1, a_3, \ldots)$. Without loss of generality assume that

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \ldots$$

Since $q_1 = \gcd(a_1, a_2) \in (a_1, a_2)$ we have that $(q_1) = (a_1, a_2)$ and by induction

$$(a_1) \subsetneq (q_1) \subsetneq (q_2) \subsetneq \ldots$$

we produce an infinite increasing chain of principal ideals in R. Since R is a UFD this is a contradiction and so we must have that every ideal of R is finitely generated.

Therefore if R is a UFD that satisfies $\gcd(a, b) \in (a, b)$ for every non-zero $a, b \in R$ we have that every ideal is finitely generated. Moreover, we have shown that in this instance each ideal is principal and therefore R is a PID concluding the proof of the claim.

2. In a ring R, an element x is nilpotent if for some positive integer n, $x^n = 0$. Let $\eta(R)$ be the set of all nilpotent elements of R.

   (a) Prove that if R is commutative then $\eta(R)$ is an ideal.

   (b) Give an example of a non-commutative ring R in which $\eta(R)$ is not an ideal.

   Solution.

   (a) Since $0^2 = 0$ we have that $0 \in \eta(R)$. Suppose that $x, y \in \eta(R)$; by assumption there exist $n, m \in \mathbb{N}$ such that $x^n = 0 = y^m$. Then

   $$(-x)^n = (-1)^n x^n = (-1)^n 0 = 0$$

   and so $-x \in \eta(R)$ (we can easily deal with the case when R does not have a unit by recalling that $(-a)^2 = a^2$ in general). Since R is commutative we can apply the binomial theorem to $(x + y)^{n+m}$ and we have

   $$(x + y)^{n+m} = \sum_{j}^{n+m} \binom{nm}{k} x^{n+m-k} y^k = 0$$

   becuase $x^{n+m-k} = 0$ for all $1 \leq k \leq m$ and $y^k = 0$ for $m \leq k \leq n + m$. This shows that $x + y \in \eta(R)$ and so $\eta(R)$ is an additive subgroup of R. Finally, let $r \in R$, by assumption $xr = rx$ and moreover we have

   $$(xr)^n = x^n r^n = 0 r^n = 0.$$

   Since $x \in \eta(R)$ and $r \in R$ were arbitrary we have that $\eta(R)$ is an ideal of R.

(b) Consider the non-commutative ring $M_2(\mathbb{Z})$ of 2×2 integer matrices. Consider the matrices

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Z}).$$

We have that

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

and so A, B are nilpotent. However,

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

and

$$(A+B)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

Then $A + B$ a unit therefore not nilpotent. Therefore $\eta(M_2(\mathbb{Z}))$ is not closed under addition and therefore cannot be an ideal.

3. Let A be a commutative ring. Show that a polynomial $f \in A[x]$ is invertible in $A[x]$ if and only if its constant term is invertible in A and the rest of its coefficients are nilpotent.

Lemma. [Dummit and Foote, Section 7.1 exercise 14.]

Let R be a commutative ring and $x \in R$ nilpotent, then

(a) $x = 0$ or x is a zero divisor

(b) rx is nilpotent for all $r \in R$

(c) $1 + x$ is a unit in R

(d) $u + n$ is a unit in R for all units u and nilpotent elements n

Proof.

(a) If $x = 0$ we're done. Otherwise let $n \in \mathbb{N}$ be the smallest integer such that $x^n = 0$. Then $x^{n-1}, x \neq 0$; however, $0 = x^n = xx^{n-1}$ and so x is a zero divisor.

(b) We proved that rx is nilpotent for all $r \in R$ in Problem 2.

(c) Claim $1 + x$ is a unit in R. Indeed, consider

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

Since we have an explicit inverse $(1+x)$ is a unit. (Note that if R is a ring without 1, by we use the notation $(-1)^k$ formally to indicate whether or not to add an element or its additive inverse.)

(d) Let $u \in R^\times$ be a unit and $n \in R$ be nilpotent. Then we have that

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

where $u^{-1}n$ is nilpotent by (b) and $1+u^{-1}n$ is a unit by (c). There exists $v \in R^\times$ such that

$$v(1+u^{-1}n) = 1 = (1+u^{-1}n)v.$$

Therefore we have that vu^{-1} is the inverse of $u+n$. Indeed

$$vu^{-1}(u+n) = v(1+u^{-1}n) = 1$$

and since R is commutative this is also a right inverse.

Solution.

Suppose that $f(x) = a_0 + a_1x + \dots a_nx^n$ is such that $a_0 \in A^\times$ is a unit and $a_1, \dots, a_n$ are nilpotent. Let $k_j \in \mathbb{N}$ be such that $a_j^{k_j} = 0$ for all $1 \le j \le n$. We show that $f(x) \in A[x]$ is a unit. Let $g(x) = f(x) - a_0$. We claim that $g(x)$ is nilpotent and then since

$$f(x) = a_0 + (f(x) - a_0)$$

we have that $f(x)$ is a unit by the lemma. Indeed, let $k = n \times \max_{1\le j\le n}\{k_j\}$ and consider $(g(x))^k$. We have

$$(g(x))^k = \sum_{\ell} \prod_{j=1}^{k} a_{\ell_j} x^{\ell_j}$$

where there are at most n distinct elements a_{ℓ_j}, $\ell_j \in \{1, \dots n\}$. This implies that for all i in the sum, there exists some j, $1 \le j \le k$, such that we have a term of the form $a_{\ell_j}^{k/n}$ and since $k/n \ge \max_{1\le j\le n}\{k_j\} \ge k_{\ell_j}$ we have that $(g(x))^k = 0$. Therefore $f(x) - a_0$ is nilpotent and as described above $f(x)$ is a unit.

Conversely, suppose that $f(x) \in A[x]$ is a unit. We show that if

$$f(x) = a_0 + a_1x + \dots a_nx^n$$

then $a_0 \in A^\times$ is a unit and $a_1, \dots, a_n$ are nilpotent.

If $\deg f = 0$ then $f(x) = a_0 \in A[x]^\times$ if and only if $a_0 \in A^\times$. Suppose that $\deg f = n > 0$ and so $a_n \neq 0$. By hypothesis there exists $g(x) = b_0 + b_1x + \dots + b_mx^m \in A[x]^\times$, $b_m \neq 0$, such that

$$f(x)g(x) = 1 = g(x)f(x) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_ib_jx^{i+j}.$$

Then we must have that $a_0b_0 = 1$ and so $a_0 \in A^\times$ is a unit. We also have that the coefficients of x^k for $1 \le k \le n+m$ are zero. In particular, we have that the coefficient of x^{n+m} is zero, i.e., $a_nb_m = 0$. Consider the coefficient of x^{n+m-1}, namely

$$a_{n-1}b_m + a_nb_{m-1} = 0$$

multiplying through by a_n we have that

$$0 = a_{n-1}a_nb_m + a_n^2b_{m-1} = a_{n-1}0 + a_n^2b_{m-1} = a_n^2b_{m-1}.$$

Similarly if we consider the coefficient of x^{n+m-2} we have

$$0 = a_{n-1}b_{m-1} + a_nb_{m-2} + a_{n-2}b_m$$

multiplying through by a_n^2 we have

$$0 = a_{n-1}(a_n)^2b_{m-1} + a_n^3b_{m-2} + (a_{n-2}a_n)a_nb_m = (a_{n-1})0 + a_n^3b_{m-2} + (a_{n-2}a_n)0 = a_n^3b_{m-2}.$$

Continuing this way we obtain

$$a^{m+1}b_0 = 0$$

but since $b_0 \in A^\times$ is a unit we must have that a_n is nilpotent. Therefore we have that

$$(f(x) - a_nx^n)g(x) = 1 - a_nx^ng(x)$$

where $a_nx^ng(x)$ is nilpotent since every coefficient is nilpotent (by the argument above). Therefore by the lemma $1 - a_nx^ng(x) = f(x)$ is a unit. By induction $a_{n-1}, ..., a_1$ are nilpotent.

This completes the proof of the claim.

4. Show that the ring $\mathbb{Z}[i] = \{a + ib \,|\, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a PID and hence a UFD. What are the units of this ring?

Solution.

We prove the stronger claim that $\mathbb{Z}[i]$ is in fact a Euclidean domain and therefore a PID, and hence UFD. First we note that $\mathbb{Z}[i]$ is commutative, has no zero divisors and is therefore an integral domain with identity $1 \neq 0$.

Define a function $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ by

$$N(0) = 0 \text{ and } N(a + ib) = a^2 + b^2,$$

(note that this is just the restriction of the complex modulus to $\mathbb{Z}[i]$). Note that N is in fact multiplicative; indeed, if $a + ib, c + id \in \mathbb{Z}[i]$ we have

$$\begin{aligned} N[(a+ib)(c+id)] &= N(ac - bd + i(ad + bc)) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2acbdb^2d^2 + a^2d^2 + 2acbd + b^2c^2 \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= N(a + ib)N(c + id), \end{aligned}$$

and certainly this property holds for the case when $a+ib = 0$ as well. The multiplicative property of N allows us to easily characterize the units of $\mathbb{Z}[i]$. Suppose that $\alpha \in \mathbb{Z}[i]$ is a unit, then we have that

$$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}),$$

since $N(\alpha), N(\alpha^{-1}) \in \mathbb{N}$ this implies that we must have $N(\alpha) = N(\alpha^{-1}) = 1$. Therefore we have that $\alpha \in \{\pm 1, \pm i\}$ and this set exhausts all units of $\mathbb{Z}[i]$.

We now show that N is a Euclidean norm. Let $\alpha = a + ib, \beta = c + id \in \mathbb{Z}[i] \setminus \{0\}$. We will show that there exists $\gamma, r \in \mathbb{Z}[i]$ with $\alpha = \gamma\beta + r$ and $N(r) \leq N(\beta)$. For a moment, consider the result of dividing α by β in $\mathbb{C}$, we will obtain rational coefficients as follows:

$$\frac{\alpha}{\beta} = \frac{a+ib}{c+id} = \left(\frac{a+ib}{c+id}\right)\left(\frac{c-id}{c-id}\right) = x + iy$$

where

$$x = \frac{ac+bd}{c^2+d^2} \quad \text{and} \quad y = \frac{bc-ad}{c^2+d^2} \in \mathbb{Q}.$$

Let $p, q \in \mathbb{Z}$ be integers such that $|x - p| \leq 1/2$ and $|y - q| \leq 1/2$. We claim that

$$\alpha = (p + iq)\beta + r \qquad \text{where } N(r) \leq \frac{1}{2}N(\beta) < N(\beta).$$

Let $\theta = (x - p) + i(y - q) \in \mathbb{Q}[i]$ and set $r = \theta\beta$ then we have

$$r = \theta\beta = ((x-p) + i(y-q))\beta = (x+iy)\beta - (p+iq)\beta = \alpha - (p+iq)\beta,$$

therefore we have $r \in \mathbb{Z}[i]$. Moreover, since N is well defined (and multiplicative) on $\mathbb{C}$ we have that

$$N(\theta) = (x-p)^2 + (y-q)^2 = |x-p|^2 + |y-q|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

and so

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

as claimed.

This proves that $\mathbb{Z}[i]$ is a Euclidean domain and therefore a PID, and hence UFD, as claimed.

5. In $\mathbb{Z}[i]$ find the greatest common divisor of 85 and $1 + 13i$, and express it as a linear combination of these two elements.

Solution.

We follow the proof above that $\mathbb{Z}[i]$ is a Euclidean domain and naively divide in $\mathbb{C}$ first. Notice that $N(85) > N(1 + 13i)$ so we will consider

$$\frac{85}{1+i13} = \left(\frac{85}{1+i13}\right)\left(\frac{1-i13}{1-i13}\right) = \frac{85 - i1105}{170} = \frac{1}{2} - i\frac{13}{2}.$$

Let $p = 1$ and $q = -7$ and set

$$\theta = \left(\frac{1}{2} - 1\right) + i\left(-\frac{13}{2} + 7\right)$$

Let $r = \theta(1+i13)$ so we have

$$r = \left(\left(\frac{1}{2}-1\right)+i\left(-\frac{13}{2}+7\right)\right)(1+i13) = 85-(1-i7)(1+i13) = -7-i6,$$

i.e., we have that

$$85 = (1-i7)(1+i13)+(-7-i6)$$

Then, since we have a division algorithm in $\mathbb{Z}[i]$, we have that

$$\gcd(85, 1+i13) = \gcd(1+i13, -7-i6).$$

We have $N(-7-i6) < N(1+i13)$, and notice that $\gcd(1+i13, -7-i6) = -7-i6$. Indeed,

$$\frac{1+i13}{-7-i6} = \left(\frac{1+i13}{-7-i6}\right)\left(\frac{-7+i6}{-7+i6}\right) = \frac{-85-i85}{85} = -1-i,$$

and so $(1+i13) = (-7-6i)(-1-i)$.

Therefore we conclude that $\gcd(85, 1+i13) = -7-i6$ (up to a unit) and we can write the gcd as a linear combination as follows

$$85-(1-i7)(1+i13) = -7-i6.$$

6. Show that the quotient ring $\mathbb{Q}[x,y]/(x^2+y^2-1)$ is not a UFD.

Lemma.

Let R be a commutative ring and $a, b \in R$, then if we consider the ideal generated by $[b] \in R/(a)$ we have that

$$(R/(a))\,/([b]) \cong R/(a,b)$$

Proof.

By the fourth isomorphism theorem for rings there is a bijection between ideals of $R/(a)$ and ideals of R containing (a). We claim that in fact $([b]) = (a,b)/(a)$. By definition, for $[b] \in R/(a)$, we have

$$([b]) = \{[x][b] \mid [x] \in R/(a)\}.$$

Let $[x] = x+(a) \in R/(a)$ then we have

$$[x][b] = (x+(a))(b+(a)) = xb + x(a) + b(a) + (a) = xb + (a) \in (a,b)/(a),$$

where

$$(a,b)/(a) = \{xa + yb + (a) \mid x, y \in R\} = \{yb + (a) \mid y \in R\}.$$

This implies that $([b]) \subset (a,b)/(a)$.

Given $yb + (a) \in (a,b)/(a)$ we have that

$$(yb + (a)) = (y+(a))(b+(a)) \in ([b]).$$

Now we have that $(a,b)/(a) \subset ([b])$.

Therefore $([b]) = (a,b)/(a)$ and so by the third isomorphism theorem for rings we have

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

as claimed.

Notation.

The notation $[\,\cdot\,]$ will denote an equivalence class in the quotient ring

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

otherwise, we will use a subscript to denote the ideal with which we are taking a quotient.

Solution.

We know that in a UFD an element is irreducible if and only if it is prime. We claim that $[x] \in \mathbb{Q}[x,y]/(x^2+y^2-1)$ is irreducible but not prime.

First we show that $[x]$ cannot be prime. If $[x]$ was a prime element then we would have that the quotient ring

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

is an integral domain. However, by the lemma we have that

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

In the ring $\mathbb{Q}[y]/(y^2-1)$ the elements $[y+1]_{(y^2-1)}$ and $[y-1]_{(y^2-1)}$ are both non-zero; however,

$$[y+1]_{(y^2-1)}[y-1]_{(y^2-1)} = [y^2-1]_{(y^2-1)} = [0]_{(y^2-1)}.$$

Since the quotient ring $\mathbb{Q}[y]/(y^2-1)$ has zero divisors it is not an integral domain and therefore $([x]) \subset \mathbb{Q}[x,y]/(x^2+y^2-1)$ is not a prime ideal. We conclude that the element $[x] \in \mathbb{Q}[x,y]/(x^2+y^2-1)$ is not prime.

Finally we show that $[x] \in \mathbb{Q}[x,y]/(x^2+y^2-1)$ is irreducible which will complete the proof. First we remark that (x) is a prime ideal of the ring $\mathbb{Q}[x,y]$ since $Q[x,y]/(x) \cong \mathbb{Q}[y]$ is an integral domain. The primality of x is somehow lost when passing to the quotient $\mathbb{Q}[x,y]/(x^2+y^2-1)$; however, we claim that $[x]$ remains irreducible.

Suppose that $[x] = [p(x,y))][q(x,y)] = [p(x,y)q(x,y)]$ is a factorization of $[x]$ in $\mathbb{Q}[x,y]/(x^2+y^2-1)$; we claim that either $p(x,y)$ or $q(x,y)$ is a unit. Then we must have that

$$x - p(x,y)q(x,y) \in (x^2+y^2-1),$$

i.e.,

$$x - p(x,y)q(x,y) = r(x,y)(x^2+y^2-1)$$

for some polynomial $r(x,y) \in Q[x,y]$. ... I'm sure $[x]$ is irreducible, but it is unclear how to proceed.