Algebra Assignment 4

Vanessa Foster

Nov 29 2011

1

Prove that a ring R is a PID iff it is a UFD in which $gcd(a,b) \in < a,b >$ for every non-zero $a,b \in R$

One direction is clear since every PID is a UFD and in a PID $< a,b >=< gcd(a,b) >$ so $gcd(a,b) \in < a,b >$ for all non-zero $a,b \in R$.
For the converse direction we need to show that R is a PID.
We will show that in R every ideal is principal, that is, every ideal is generated by a single element. First we consider the ideal I generated by a finite number of distinct elements, $I =< n_1, n_2, \ldots, n_k >$ with $n_1, n_2, \ldots, n_k \in R$. Then, (using property that, $gcd(a,b) \in < a,b >$ for every non-zero $a,b \in R$)

$$\begin{aligned} < n_1, n_2, \ldots, n_k > &=< gcd(n_1, n_2), n_3, \ldots, n_k > \\ &=< gcd(gcd(n_1, n_2), n_3), n_4, \ldots, n_k > \\ &\vdots \\ &=< gcd(\ldots gcd(gcd(gcd(n_1, n_2), n_3), n_4) \ldots, n_k) > \end{aligned}$$

and let $gcd(\ldots gcd(gcd(gcd(n_1, n_2), n_3), n_4) \ldots, n_k) = q$. Therefore,$< n_1, n_2, \ldots, n_k >=< q >$ and we have shown that any ideal in R generated by a finite number of distint elements can be written as an ideal generated by one element.
Next, we need to deal with the case where an ideal in our UFD R is generated by an infinite number of distinct elements. However, we claim that there are no ideals generated by an infinite number of elements.
We will prove this by contradiction. We assume that there exists an ideal I_∞ such that I_∞ is generated by infinitely many elements of R.
claim(1): A UFD satisfies the ascending chain condition.
If $< a_1 > \subsetneq < a_2 > \subsetneq < a_3 > \subsetneq \ldots$ is an ascending chain of principal ideals (inclusions being strict) then for some $N \in \mathbb{N}$ $\quad < a_N >=< a_{N+1} >= \ldots$.

This is holds since we are in a UFD and so every a_i which generates a principal ideal decomposes into a unique (up to a unit) prime factorization. Since $< a_1 > \subsetneq < a_2 >$ then there must be some prime factor in $a_1 = p_1 p_2 \dots p_m$ which is not in $a_2 = p_1 p_2 \dots p_{m-1}$ so continuing in this manner, for some $N \in \mathbb{N}$,

$$< a_1 = p_1 p_2 \dots p_m > \subsetneq < a_2 = p_1 p_2 \dots p_{m-1} > \subsetneq \cdots \subsetneq < a_N = p_1 u > = < a_{N+1} = u a_N > = \dots$$

where u is a unit ($u \in R^\times$).
claim (2): If I_∞ is infinitely generated, the ascending chain condition fails to hold on R.
Let I_∞ be an ideal generated by infinitely many elements. Using I_∞ we will create an ascending chain which violates the ascending chain condition. Let $b_1 = a_1$ and notice that $I_\infty \backslash < a_1 > \neq \varnothing$ is non-empty because I_∞ is generated by infinitely many elements. Next, we choose $b_2 \in I_\infty \backslash < a_1 >$ and we define $c_1 = gcd(b_1, b_2)$. Then, continuing this way...

$$< b_1 > \subsetneq < c_1 > \subsetneq < c_2 > \subsetneq \dots$$

This ascending chain will never repeat for some N because $I_\infty \backslash < c_i > \neq \varnothing$ for all c_i because I_∞ is generated by infinitely many elements.
Since we have shown that some infinitely generated ideal I_∞ violates the ascending chain condition, this proves that there are no infinitely generated ideals in R. Then we are reduced to our first case of finitely generated ideals which we already showed can be expressed as principal ideals. Therefore, we have shown that every ideal in R is principal, proving that R is a PID.

2

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

1. *Prove that if R is commutative then $\eta(R)$ is an ideal.*
2. *Give an example of a non-commutative ring R in which $\eta(R)$ is not an ideal.*

Part 1
First we need to show that $\eta(R)$ is an additive subgroup of R.
It is obvious that $0 \in \eta(R)$. For $x, y \in \eta(R)$ we need to show that $x + y \in \eta(R)$. Let $x^n = 0$ and $y^m = 0$ and with out loss of generality assume that $n < m$, we need to find a p such that $(x+y)^p = 0$. Let $p = mn$, then $(x+y)^p = \sum_{i=0}^{p} \begin{pmatrix} p \\ i \end{pmatrix} x^{p-i} y^i$ and for $i = 0, n, m, p$ it is clear that $x^{p-i} y^i = 0$. Then, for $i < n$ $x^{nm-i} = 0$, and $n < i < m$, $m < i$, $x^{nm-i} y^i = 0$. Therefore, $(x+y)^p = 0$ and $(x+p) \in \eta(R)$. Next, we need to show that $x \in \eta(R) \implies \exists x^{-1} \in \eta(R)$ such that $x + x^{-1} = 0$. For $x \in < R, +, 0 > \exists x^{-1} \in R$

such that $x^{-1} + x = 0 = x + x^{-1}$. So it remains to show that for some m, $(x^{-1})^m = 0$. $x^{-1} + x = 0 = x^n \implies x^{-1} = x^n - x \implies (x^{-1})^n = (x^n - x)^n$, then as done above, we can use the binomial expansion $(x^n - x)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i (x^n)^{n-i} x^i$ and so $(x^{-1})^n = 0$ as required. Next, we will show that for every $r \in R$, $rx \in \eta(R)$ and $xr \in \eta(R)$.
$x \in \eta(R) \implies x^n = 0$ some $n > 0$ and so $(rx)^n = (rx) \dots (rx)$ n times, but since R is commutative, $(rx)^n = r^n x^n = 0x^n = 0$ so $rx \in \eta(R)$. By the same method, $xr \in \eta(R)$ also.

Part 2
We will use the non-commutative ring, $M_{2\times 2}(\mathbb{Z})$ as our counter example. It is clear that elements in $A, B \in \eta(M_{2\times 2}(\mathbb{Z}))$ where

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $A^2 = B^2 = 0$. However, $\eta(M_{2\times 2}(\mathbb{Z}))$ is not an ideal, since it fails to be an additive subgroup. $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $(A + B) \notin \eta(M_{2\times 2}(\mathbb{Z}))$ because $(A + B)^2 = Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and for all n, the $(Id)^n \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

3

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

First we assume that a_0 is invertible in A and all other coefficients of $f(x)$ are nilpotent.

Conversely, we assume that $f(x)$ is invertible in $A[x]$ and prove that the constant term is invertible and that the rest of the coefficients of $f(x)$are nilpotent.
$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ invertible in $A[x] \implies \exists g(x) \in A[x]$ $(g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$, where wlog we assume $n \leq m)$ such that $f(x)g(x) = 1$. Since A is a commutative ring we can use the evaluation ring homomorphism at $x = 0$,

$$ev_{x=o} : A[x] \to A \text{ where } (f(x)m(x)) = (1)_{A[x]} \mapsto (f(0)g(0)) = (a_0 b_0) = (1)_A$$

So we have shown that the constant term a_0 of $f(x)$ is invertible in A. Now, we need to show that $a_i \in \eta(A)$ for all coefficients of $f(x)$ where $i \geq 1$. We will show this using two induction steps.
First,

$$\begin{aligned} 1 &= f(x)g(x) \\ &= (a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n)(b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m) \\ &= a_0 b_0 + a_0 b_1 x + \cdots + a_0 b_m x^m + a_1 b_0 x + \cdots + a_1 b_m x^{m+1} + \cdots + \cdots + a_n b_m x^{n+m} \end{aligned}$$

So, $0 = 1 - a_0b_0 = a_0b_1x + \cdots + a_0b_mx^m + a_1b_0x + \cdots + a_1b_mx^{m+1} + \cdots + \cdots + a_nb_mx^{n+m}$. Then, $a_nb_m = 0$ and so, $a_{n-1}b_m + a_nb_{m-1} = 0 \implies a_n(a_{n-1}b_m + a_nb_{m-1}) = a_na_{n-1}b_m + a_n^2b_{m-1} = 0 \implies a_n^2b_{m-1} = 0$ continuing this way ... $\implies a_n^{n+1}b_0 = 0$ and since b_0 is a unit, we get that $(a_n)^{n+1} = 0$ (ie: a_n is nilpotent). Furthermore,

$$f(x)g(x) = [\big(f(x) - a_nx^n\big) + a_nx^n]g(x)$$
$$1 = (f(x) - a_nx^n)g(x) + a_nx^ng(x)$$

So, $(f(x) - a_nx^n)g(x) = 1 - a_nx^ng(x)$. Where $1 - a_nx^ng(x)$ is a polynomial where all the coefficients except the first are nilpotent (since a_n is nilpotent). Therefore by what we showed above, the polynomial $1 - a_nx^ng(x)$ is a unit. Now we can use a second induction argument on n which proves that all other coefficients of $f(x)$ (except a_0) are nilpotent as desired.

4

Show that the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a PID and hence a UFD. What are the units of that ring?
We will show that $\mathbb{Z}[i]$ is a Euclidean Domain and use that $\mathbb{Z}[i]$ a euclidean domain $\implies$ $\mathbb{Z}[i]$ is a PID $\implies$ $\mathbb{Z}[i]$ is a UFD.
Claim: $\mathbb{Z}[i]$ is a Euclidean Domain.
Proof: We need to show that there is a norm $N(\cdot)$ ($N : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N}$) on $\mathbb{Z}[i]$ such that the following conditions hold:

1. $N(z_1z_2) \geq N(z_1)$ and $N(z_1z_2) \geq N(z_2)$ for all $z_1, z_2 \in \mathbb{Z}[i]$
2. For all $z_1, z_2 \in \mathbb{Z}[i] - \{0\}$, $\exists q, r \in \mathbb{Z}[i]$ such that $z_1 = z_2q + r$ and either $r = 0$ or $N(r) < N(z_2)$

For $z_1 = a + bi, z_2 = c + di \in \mathbb{Z}[i]$, we define our norm N to be $N(z_1 = a + bi) = a^2 + b^2$. Then, $N(z_1z_2) = (ac - bd)^2 + (ad - bc)^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) > a^2 + b^2 = N(z_1)$ and the similarly for $N(z_1z_2) > N(z_2)$.
Next, with $z_1 = a + bi, z_2 = c + di \in \mathbb{Z}[i]$ ($z_2 \neq 0$), we get that $\dfrac{z_1}{z_2} = \alpha + \beta i$ where $\alpha = \dfrac{(ac + bd)}{c^2 + d^2}$, $\beta = \dfrac{(bc - ad)}{c^2 + d^2}$ and $\alpha, \beta \in \mathbb{Q}$. Then we let

$$\begin{cases} m \in \mathbb{Z} \text{ where } m \text{ is closest to } \alpha \in \mathbb{Q} & \text{such that} |\alpha - m| < \frac{1}{2} \\ n \in \mathbb{Z} \text{ where } n \text{ is closest to } \beta \in \mathbb{Q} & \text{such that } |\beta - n| < \frac{1}{2} \end{cases}$$

Now, we need to show that $z_1 = (m + ni)z_2 + z_3$ for some $z_3 \in \mathbb{Z}[i]$ with $N(z_3) \leq \frac{1}{2}N(z_2)$. Moreover, if we set $Z = (\alpha - m) + (\beta - n)i$ and $z_3 = z_2Z$ then we get that $z_3 = z_1 - (m + ni)z_2$ so $z_3 \in \mathbb{Z}[i]$ and then $z_1 = (m + ni)z_2 + z_3$. Finally, since $N(Z) = (\alpha - m)^2 + (\beta - n)^2 = (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$, then $N(z_3) = N(Z)N(z_2) \leq \frac{1}{2}N(z_2)$.
And this shows that the Euclidean Algorithm holds for $\mathbb{Z}[i]$ as required. It is clear that the units in $\mathbb{Z}[i]$ are$\{\pm 1, \pm i\}$ since these are the only elements in $\mathbb{Z}[i]$ which have an inverse.

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.

Since we know that $\mathbb{Z}[i]$ is a euclidean domain we will use the Euclidean Algorithm to find $gcd(85, 1+13i)$.

$$85 = (1+13i)(-6i) + (7+6i)$$
$$(1+13i) = (7+6i)(i+1) + 0$$

Thus, $(1+13i) = (7+6i)(i+1)$, $85 = (7+6i)(i+1)(-6i) + (7+6i) = (7+6i)(7+6i)$ and $gcd(85, 1+13i) = (7+6i)$. Expressing this as a linear combination of 85 and $(1+13i)$:

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

6

(Hard!) Show that the quotient ring $\mathbb{Q}[x,y]/ < x^2+y^2-1 >:= R$ is not a UFD.

First we notice that in R, $[x^2+y^2-1] = [0] \implies [x^2] = [1-y^2] \implies [x^2] = [1+y][1-y] \implies [x][x] = [1+y][1-y]$. So if we can show that $[x], [1-y]$ and $[1+y]$ are irreducible, we can deduce that $[x^2]$ has two distinct factorizations in R implying that R cannot be a UFD. By the following theorem: *R is a UFD $\iff$ every non-zero element of R has a unique decomposition into irreducibles.*
Therefore we we need to show that $[1-y], [1+y]$ are irreducible in R...