Algebra II: Homework 1

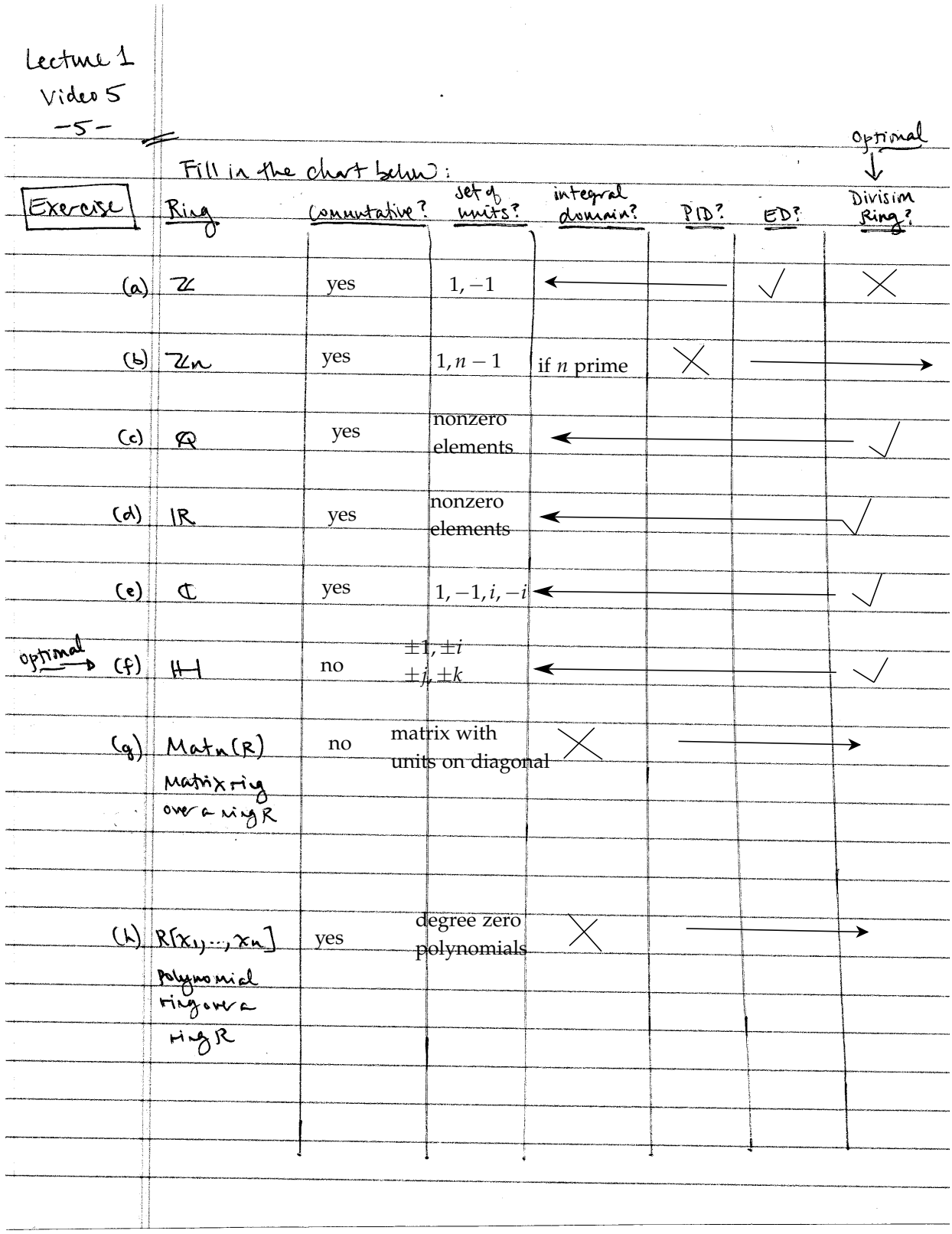
Due on February 03, 2021

Professor Walton

Gabriel Gress

Last edited February 3, 2021

Problem 1



Lecture 1
Video 5
-5-

Fill in the chart below:

Exercise	Ring	Commutative?	Set of units?	Integral domain?	PID?	ED?	Optimal: Division Ring?
(a)	$\mathbb{Z}$	yes	$1, -1$	←	←	✓	✗
(b)	$\mathbb{Z}_n$	yes	$1, n-1$	if n prime	✗	→	→
(c)	$\mathbb{Q}$	yes	nonzero elements	←	←	←	✓
(d)	$\mathbb{R}$	yes	nonzero elements	←	←	←	✓
(e)	$\mathbb{C}$	yes	$1, -1, i, -i$	←	←	←	✓
optimal → (f)	$\mathbb{H}$	no	$\pm 1, \pm i$ $\pm j, \pm k$	←	←	←	✓
(g)	$\mathrm{Mat}_n(R)$ Matrix ring over a ring R	no	matrix with units on diagonal	✗	→	→	→
(h)	$R[x_1, \ldots, x_n]$ Polynomial ring over a ring R	yes	degree zero polynomials	✗	→	→	→

Problem 1 continued on next page...
Figure 1: Worksheet 1

Problem 2

Claim. Let R be a UFD.

(a). Let b and $a_1, \dots, a_s$ be nonzero elements of R. For $d \in R$, show that

$$bd = gcd(ba_1, \dots, ba_s) \iff d = gcd(a_1, \dots, a_s)$$

(b). Let $f(x) \in R[x]$ where $f(x) = bf_1(x)$ for $f_1(x)$ **primitive** (i.e. $gcd(\text{coefficients of } f_1(x)) = 1_R$). Show that

$$b = gcd(\{\text{coefficients of } f(x)\}).$$

Proof. (a). First, assume that $bd = gcd(ba_1, \dots, ba_s)$. Now consider an arbitrary d' that satisfies

$$d' \mid a_1, \dots, a_s.$$

We want to show that $d' \mid d$. Observe that if $d' \mid a_1, \dots, a_s$, then $d' \mid ba_1, \dots, ba_s$, as the prime factorization of ba_i trivially contains the prime factorization of a_i. This then implies that $d' \mid bd$ by hypothesis. But we know that $bd' \mid ba_i$ and hence $bd' \mid bd$. This only holds if $d' \mid d$, as desired.

For the reverse direction, assume that $d = gcd(a_1, \dots, a_s)$. First, observe that $bd \mid ba_1, \dots, ba_s$. Thus it only remains to show that if $d' \mid ba_1, \dots, ba_s$, then $d' \mid bd$. Assume for a contradiction that d' cannot be factored as bd''. Then there exists a factor of b such that $b_i d' \mid ba_1, \dots, ba_s$. Of course, if $b_i d'$ divides a term, then d' divides a term. In other words, we can simply look at the case where bd'' exists, as if it doesn't, then we can multiply it by prime factors until it does, and division will still hold. Now we consider bd''. Of course, if $bd'' \mid ba_i$, then $d'' \mid a_i$. Then we know that $d'' \mid d$ by hypothesis, in which case $bd'' \mid bd$, as desired.

□

Problem 3

Claim.

(a). Let R be a commutative ring with identity 1. Show that the polynomial rings $R[x_1, \dots, x_{n-1}, x_n]$ and $R[x_1, \dots, x_{n-1}][x_n]$ can be identified.

(b). Show by induction that if K is a field, then, for all n, $K[x_1, \dots, x_{n-1}, x_n]$ is a unique factorization domain.

Proof. Let $C_{\alpha_1 \dots \alpha_n}$ be the coefficient of $x^{\alpha_1} \dots x^{\alpha_n}$ in $R[x_1, \dots x_n]$. Let $\varphi : R[x_1, \dots x_n] \to R[x_1, x_{n-1}][x_n]$ be given by

$$\varphi\left(\sum_{(\alpha_1, \dots \alpha_n) \in \mathbb{N}} C_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}\right) = \sum_{j \in \mathbb{N}} \left(\sum_{\alpha_1, \dots \alpha_{n-1}} C_{\alpha_1 \dots \alpha_n} x_1^{\alpha_1} \dots x_{n-1}^{\alpha_{n-1}}\right) x_n^{\alpha_j} \tag{1}$$

Problem 3 continued on next page...

One can observe that φ is the identity map on elements with no x_n term, and clearly one-to-one for elements with x_n, and hence an isomorphism. The proof of part (b) is by induction. The base case $n = 1$ is given by Theorem 6.6.7. Then suppose the result holds for a nonnegative integer n. Then by induction hypothesis,

$$F[x_1, ...x_n]$$

is a UFD. By part (a), we have

$$F[x_1...x_{n+1}] \cong F[x_1, ...x_n][x_{n+1}] \tag{2}$$

which is a UFD by Theorem 6.6.7. □

Problem 4

Claim. Use Gauss' lemma to show that if a polynomial $a_n x^n + \ldots + a_1 x + a_0 \in Z[x]$ has a rational root r/s, where r and s are relatively prime, then $s \mid a_n$ and $r \mid a_0$. In particular, if the polynomial is monic, then its only rational roots are integers.

Proof. Because $\mathbb{Z}$ is a UFD, we can apply Gauss' Lemma. Then if a polynomial has a rational root r/s, we know by a proposition in class that it has a degree 1 factor in $F[x]$. Hence it is reducible in $F[x]$, which by Gauss' Lemma implies that it is reducible in $R[x]$. Of course, in order for r/s to give a degree 1 factor in both domains, it must hold that the factor is in R and hence in Z, and so in order for this to hold we can assure that $s \mid a_0$ and $r \mid a_0$, so that the rational roots are integers.

□

Problem 4 continued on next page...

Problem 5

Claim. Complete the details of this alternative proof of Gauss' Lemma:

Let R be a UFD. For any irreducible $p \in R$, consider the quotient map $\pi_p : R \to R/pR$, and extend this to a homomorphism $\pi_p : R[x] \to (R/pR)[x]$, defined by $\pi_p(\sum a_i x^i) = \sum_i \pi_p(a_i)x^i$, using Corollary 6.2.9.

(a). Show that a polynomial $h(x)$ is in the kernel of π_p if and only if p is a common divisor of the coefficients of $h(x)$.

(b). Show that $f(x) \in R[x]$ is primitive if and only if for all irreducible p, $\pi_p(f(x)) \neq 0$.

(c). Show that $(R/pR)[x]$ is integral domain for all irreducible p.

(d). Conclude that if $f(x)$ and $g(x)$ are primitive in $R[x]$, then $f(x)g(x)$ is primitive as well.

Proof. (a). First, assume that $h(x)$ is in the kernel of π_p, that is, $\pi_p(h(x)) = 0$. Note that in order for this to be zero, each $\pi_p(a_i)$ must be identically zero, as you cannot simplify $x^i + x^j$ for $i \neq j$. This only occurs if a_i is zero in R/pR, which implies it is divisible by p because all ideals are prime ideals in R. If instead every a_i is divisible by p, then a_i must map to 0 in R/pR and so π_p maps $h(x)$ to a sum with all coefficients zero, and hence $\pi_p(h(x)) = 0$.

(b). Assume that there is an irreducible p such that $\pi_p(f(x)) = 0$. Then by the first part, p divides all coefficients, and hence can factor from $f(x)$, so it wouldn't be primitive. That shows that if $f(x)$ is primitive, there cannot exist such a p. Now assume that for all irreducible p, $\pi_p(f(x)) \neq 0$. Because R is a UFD, there exists a unique prime factorization for all a_i. Because of the hypothesis, there cannot be a prime shared by all elements, otherwise it would be zero in the homomorphism. Then the set of coefficients share no prime factors, and hence the greatest common divisor must be 1, giving us that $f(x)$ is primitive.

(c). Consider

$$\left(\sum \pi_p(a_i)x^i\right)\left(\pi_p(a_i')x'^i\right) = \sum\sum \pi_p(a_i)\pi_p(a_j')x^i x'^j.$$

Observe that in order for this to be zero, we require $a_i a_j' + a_j a_i' = 0$ for all i, j. If p is irreducible, then we know that this implies that each term in the sum must have a zero. We will show that both terms must in fact be zero. Assume that a_i is zero, so that $a_i a_j'$ is zero. If the first polynomial is non-zero, then there exists an a_k that is non-zero, and hence $a_k a_j'$ would be positive. But then we wouldn't have all sums zero, so there is a contradiction. Thus, if any a_i or a_j' is nonzero, then the other must be zero for all terms. This implies that one or both of the polynomials must be identically zero, and hence there are no zero divisors.

(d). As expanded above, our coefficients for $f(x)g(x)$ can be expressed by $a_i a_j' + a_j a_i'$. This sum has a prime factorization– assume for a contradiction that there is a p_i that factors out from all the sums. Then p_i must also divide each $a_i a_j'$ AND $a_j a_i'$. If it doesn't divide either of a_i, a_j, then it must divide every a_i', and so $g(x)$ couldn't have been primitive. Otherwise, it will divide either a_i or a_j for each i, j, and eventually will divide each element, giving that $f(x)$ couldn't have been primitive. Ergo, the product cannot have a gcd that is non-unital, and hence it is primitive, as desired.

□

Problem 5 continued on next page...