Lecture 1

1.1 Definition of Rings and Examples

A ring will be a set of elements, R, with both an **addition** and **multiplication** operation satisfying a number of "natural" axioms.

Axiom 1.1 (Axioms for a ring) *Let R be a set with 2 binary operations called addition (written $a+b$) and multiplication (written ab). R is called a* ***ring*** *if for all $a, b, c \in R$ we have*

1. $(a+b)+c = a+(b+c)$
2. *There exists an element $0 \in R$ which is an identity for $+$.*
3. *There exists an element $-a \in R$ such that $a+(-a) = 0$.*
4. $a+b = b+a$.
5. $(ab)c = a(bc)$.
6. $a(b+c) = ab+ac$ *and* $(b+c)a = ba+bc$.

Items 1. – 4. are the axioms for an abelian group, $(R,+)$. Item 5. says multiplication is associative, and item 6. says that is both left and right distributive over addition. Thus we could have stated the definition of a ring more succinctly as follows.

Definition 1.2. *A* ***ring*** *R is a set with two binary operations "$+$" = addition and "$\cdot$"= multiplication, such that $(R,+)$ is an abelian group (with identity element we call 0), "$\cdot$" is an associative multiplication on R which is both left and right distributive over addition.*

Remark 1.3. The multiplication operation might not be commutative, i.e., $ab \neq ba$ for some $a, b \in R$. If we have $ab = ba$ for all $a, b \in R$, we say R is a **commutative ring**. Otherwise R is **noncommutative.**

Definition 1.4. *If there exists and element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$, then we call 1 the* ***identity element*** *of R [the book calls it the unity.]*

Most of the rings that we study in this course will have an identity element.

Lemma 1.5. *If R has an identity element 1, then 1 is unique. If an element $a \in R$ has a multiplicative inverse b, then b is unique, and we write $b = a^{-1}$.*

Proof. Use the same proof that we used for groups! I.e. $1 = 1 \cdot 1' = 1'$ and if b, b' are both inverses to a, then $b = b(ab') = (ba)b' = b'$. ■

Notation 1.6 (Subtraction) *In any ring R, for $a \in R$ we write the additive inverse of a as $(-a)$. So at $a+(-a) = (-a)+a = 0$ by definition. For any $a, b \in R$ we abbreviate $a+(-b)$ as $a-b$.*

Let us now give a number of examples of rings.

Example 1.7. Here are some examples of commutative rings that we are already familiar with.

1. $\mathbb{Z}$ = all integers with usual $+$ and $\cdot$.
2. $\mathbb{Q}$ = all $\frac{m}{n}$ such that $m, n \in \mathbb{Z}$ with $n \neq 0$, usual $+$ and $\cdot$. (We will generalize this later when we talk about "fields of fractions.")
3. $\mathbb{R}$ = reals, usual $+$ and $\cdot$.
4. $\mathbb{C}$ = all complex numbers, i.e. $\{a+ib : a, b \in \mathbb{R}\}$, usual $+$ and $\cdot$ operations. (We will explicitly verify this in Proposition 3.7 below.)

Example 1.8. $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ is a ring without identity.

Example 1.9 (Integers modulo m). For $m \geq 2$, $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$ with

$$\begin{aligned} + &= \text{addition} \mod m \\ \cdot &= \text{multiplication} \mod n. \end{aligned}$$

Recall from last quarter that $(\mathbb{Z}_m, +)$ is an abelian group and we showed,

$$[(ab) \bmod m \cdot c] \bmod m = [abc] = [a(bc) \bmod m] \bmod m \quad \text{(associativity)}$$

and

$$\begin{aligned} [a \cdot (b+c) \bmod m] \bmod m &= [a \cdot (b+c)] \bmod m \\ &= [ab+ac] \bmod m = (ab) \bmod m + (ac) \bmod m \end{aligned}$$

which is the distributive property of multiplication $\bmod m$. Thus $\mathbb{Z}_m$ is a ring with identity, 1.

Example 1.10. $M_2(F) = 2 \times 2$ matrices with entries from F, where $F = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ with binary operations;

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a+a' & b+b' \\ c+c' & d+d' \end{bmatrix} \text{ (addition)}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{bmatrix}. \text{ (multiplication)}$$

That is multiplication is the usual matrix product. You should have checked in your linear algebra course that $M_2(F)$ is a non-commutative ring with identity,

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

For example let us check that left distributive law in $M_2(\mathbb{Z})$;

$$\begin{aligned} &\begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} p & q \\ r & s \end{bmatrix} \right) \\ &\quad = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p+e & f+q \\ g+r & h+s \end{bmatrix} \\ &\quad = \begin{bmatrix} b(g+r)+a(p+e) & a(f+q)+b(h+s) \\ d(g+r)+c(p+e) & c(f+q)+d(h+s) \end{bmatrix} \\ &\quad = \begin{bmatrix} bg+ap+br+ae & af+bh+aq+bs \\ dg+cp+dr+ce & cf+dh+cq+ds \end{bmatrix} \end{aligned}$$

while

$$\begin{aligned} &\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} \\ &= \begin{bmatrix} bg+ae & af+bh \\ dg+ce & cf+dh \end{bmatrix} + \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix} \\ &= \begin{bmatrix} bg+ap+br+ae & af+bh+aq+bs \\ dg+cp+dr+ce & cf+dh+cq+ds \end{bmatrix} \end{aligned}$$

which is the same result as the previous equation.

Example 1.11. We may realize $\mathbb{C}$ as a sub-ring of $M_2(\mathbb{R})$ as follows. Let

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2(\mathbb{R}) \text{ and } \mathbf{i} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

and then identify $z = a + ib$ with

$$aI + b\mathbf{i} := a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Since

$$\mathbf{i}^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = I$$

it is straight forward to check that

$$\begin{aligned} (aI + b\mathbf{i})(cI + d\mathbf{i}) &= (ac - bd)\, I + (bc + ad)\, \mathbf{i} \text{ and} \\ (aI + b\mathbf{i}) + (cI + d\mathbf{i}) &= (a + c)\, I + (b + d)\, \mathbf{i} \end{aligned}$$

which are the standard rules of complex arithmetic. The fact that $\mathbb{C}$ is a ring now easily follows from the fact that $M_2(\mathbb{R})$ is a ring.

In this last example, the reader may wonder how did we come up with the matrix $\mathbf{i} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ to represent i. The answer is as follows. If we view $\mathbb{C}$ as $\mathbb{R}^2$ in disguise, then multiplication by i on $\mathbb{C}$ becomes,

$$(a, b) \sim a + ib \to i(a + ib) = -b + ai \sim (-b, a)$$

while

$$\mathbf{i} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -b \\ a \end{pmatrix}.$$

Thus $\mathbf{i}$ is the 2×2 real matrix which implements multiplication by i on $\mathbb{C}$.

Theorem 1.12 (Matrix Rings). *Suppose that R is a ring and $n \in \mathbb{Z}_+$. Let $M_n(R)$ denote the $n \times n$ – matrices $A = (A_{ij})_{i,j=1}^n$ with entries from R. Then $M_n(R)$ is a ring using the addition and multiplication operations given by,*

$$\begin{aligned} (A + B)_{ij} &= A_{ij} + B_{ij} \text{ and} \\ (AB)_{ij} &= \sum_k A_{ik} B_{kj}. \end{aligned}$$

Moreover if $1 \in R$, then

$$I := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is the identity of $M_n(R)$.

Proof. I will only check associativity and left distributivity of multiplication here. The rest of the proof is similar if not easier. In doing this we will make use of the results about sums in the Appendix 1.2 at the end of this lecture.

Let A, B, and C be $n \times n$ – matrices with entries from R. Then

$$[A(BC)]_{ij} = \sum_k A_{ik}(BC)_{kj} = \sum_k A_{ik}\left(\sum_l B_{kl}C_{lj}\right) = \sum_{k,l} A_{ik}B_{kl}C_{lj}$$

while

$$[(AB)C]_{ij} = \sum_l (AB)_{il} C_{lj} = \sum_l \left(\sum_k A_{ik}B_{kl}\right) C_{lj} = \sum_{k,l} A_{ik}B_{kl}C_{lj}.$$

Similarly,

$$[A(B+C)]_{ij} = \sum_k A_{ik}(B_{kj}+C_{kj}) = \sum_k (A_{ik}B_{kj} + A_{ik}C_{kj}) = \sum_k A_{ik}B_{kj} + \sum_k A_{ik}C_{kj} = [AB]_{ij} + [AC]_{ij}.$$

■

Example 1.13. In $\mathbb{Z}_6$, 1 is an identity for multiplication, but 2 has no multiplicative inverse. While in $M_2(\mathbb{R})$, a matrix A has a multiplicative inverse if and only if $\det(A) \neq 0$.

Example 1.14 (Another ring without identity). Let

$$R = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$$

with the usual addition and multiplication of matrices.

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

The identity element for multiplication "wants" to be $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, but this is not in R.

More generally if $(R,+)$ is any abelian group, we may make it into a ring in a trivial way by setting $ab = 0$ for all $a, b \in R$. This ring clearly has no multiplicative identity unless $R = \{0\}$ is the trivial group.

1.2 Appendix: Facts about finite sums

Throughout this section, suppose that $(R,+)$ is an abelian group, Λ is any set, and $\Lambda \ni \lambda \to r_\lambda \in R$ is a given function.

Theorem 1.15. *Let $\mathcal{F} := \{A \subset \Lambda : |A| < \infty\}$. Then there is a unique function, $S : \mathcal{F} \to R$ such that;*

1. *$S(\emptyset) = 0$,*
2. *$S(\{\lambda\}) = r_\lambda$ for all $\lambda \in \Lambda$.*
3. *$S(A \cup B) = S(A) + S(B)$ for all $A, B \in \mathcal{F}$ with $A \cap B = \emptyset$.*

Moreover, for any $A \in \mathcal{F}$, $S(A)$ only depends on $\{r_\lambda\}_{\lambda \in A}$.

Proof. Suppose that $n \geq 2$ and that $S(A)$ has been defined for all $A \in \mathcal{F}$ with $|A| < n$ in such a way that S satisfies items 1. – 3. provided that $|A \cup B| < n$. Then if $|A| = n$ and $\lambda \in A$, we must define,

$$S(A) = S(A \setminus \{\lambda\}) + S(\{\lambda\}) = S(A \setminus \{\lambda\}) + r_\lambda.$$

We should verify that this definition is independent of the choice of $\lambda \in A$. To see this is the case, suppose that $\lambda' \in A$ with $\lambda' \neq \lambda$, then by the induction hypothesis we know,

$$\begin{aligned} S(A \setminus \{\lambda\}) &= S([A \setminus \{\lambda, \lambda'\}] \cup \{\lambda'\}) \\ &= S(A \setminus \{\lambda, \lambda'\}) + S(\{\lambda'\}) = S(A \setminus \{\lambda, \lambda'\}) + r_{\lambda'} \end{aligned}$$

so that

$$\begin{aligned} S(A \setminus \{\lambda\}) + r_\lambda &= [S(A \setminus \{\lambda, \lambda'\}) + r_{\lambda'}] + r_\lambda \\ &= S(A \setminus \{\lambda, \lambda'\}) + (r_{\lambda'} + r_\lambda) \\ &= S(A \setminus \{\lambda, \lambda'\}) + (r_\lambda + r_{\lambda'}) \\ &= [S(A \setminus \{\lambda, \lambda'\}) + r_\lambda] + r_{\lambda'} \\ &= [S(A \setminus \{\lambda, \lambda'\}) + S(\{\lambda\})] + r_{\lambda'} \\ &= S(A \setminus \{\lambda'\}) + r_{\lambda'} \end{aligned}$$

as desired. Notice that the "moreover" statement follows inductively using this definition.

Now suppose that $A, B \in \mathcal{F}$ with $A \cap B = \emptyset$ and $|A \cup B| = n$. Without loss of generality we may assume that neither A or B is empty. Then for any $\lambda \in B$, we have using the inductive hypothesis, that

$$\begin{aligned} S(A \cup B) &= S(A \cup [B \setminus \{\lambda\}]) + r_\lambda = (S(A) + S(B \setminus \{\lambda\})) + r_\lambda \\ &= S(A) + (S(B \setminus \{\lambda\}) + r_\lambda) = S(A) + (S(B \setminus \{\lambda\}) + S(\{\lambda\})) \\ &= S(A) + S(B). \end{aligned}$$

Thus we have defined S inductively on the size of $A \in \mathcal{F}$ and we had no choice in how to define S showing S is unique. ∎

Notation 1.16 *Keeping the notation used in Theorem 1.15, we will denote* $S(A)$ *by* $\sum_{\lambda \in A} r_\lambda$. *If* $A = \{1, 2, \dots, n\}$ *we will often write,*

$$\sum_{\lambda \in A} r_\lambda = \sum_{i=1}^{n} r_i.$$

Corollary 1.17. *Suppose that* $A = A_1 \cup \dots \cup A_n$ *with* $A_i \cap A_j = \emptyset$ *for* $i \neq j$ *and* $|A| < \infty$. *Then*

$$S(A) = \sum_{i=1}^{n} S(A_i) \text{ i.e. } \sum_{\lambda \in A} r_\lambda = \sum_{i=1}^{n} \left(\sum_{\lambda \in A_i} r_\lambda \right).$$

Proof. As usual the proof goes by induction on n. For $n = 2$, the assertion is one of the defining properties of $S(A) := \sum_{\lambda \in A} r_\lambda$. For $n \geq 2$, we have using the induction hypothesis and the definition of $\sum_{i=1}^{n} S(A_i)$ that

$$\begin{aligned} S(A_1 \cup \dots \cup A_n) &= S(A_1 \cup \dots \cup A_{n-1}) + S(A_n) \\ &= \sum_{i=1}^{n-1} S(A_i) + S(A_n) = \sum_{i=1}^{n} S(A_i). \end{aligned}$$

∎

Corollary 1.18 (Order does not matter). *Suppose that* A *is a finite subset of* Λ *and* B *is another set such that* $|B| = n = |A|$ *and* $\sigma : B \to A$ *is a bijective function. Then*

$$\sum_{b \in B} r_{\sigma(b)} = \sum_{a \in A} r_a.$$

In particular if $\sigma : A \to A$ *is a bijection, then*

$$\sum_{a \in A} r_{\sigma(a)} = \sum_{a \in A} r_a.$$

Proof. We again check this by induction on $n = |A|$. If $n = 1$, then $B = \{b\}$ and $A = \{a := \sigma(b)\}$, so that

$$\sum_{x \in B} r_{\sigma(x)} = r_{\sigma(b)} = \sum_{a \in A} r_a$$

as desired. Now suppose that $N \geq 1$ and the corollary holds whenever $n \leq N$. If $|B| = N + 1 = |A|$ and $\sigma : B \to A$ is a bijective function, then for any $b \in B$, we have with $B' := B' \setminus \{b\}$ that

$$\sum_{x \in B} r_{\sigma(x)} = \sum_{x \in B'} r_{\sigma(x)} + r_{\sigma(b)}.$$

Since $\sigma|_{B'} : B' \to A' := A \setminus \{\sigma(b)\}$ is a bijection, it follows by the induction hypothesis that $\sum_{x \in B'} r_{\sigma(x)} = \sum_{\lambda \in A'} r_\lambda$ and therefore,

$$\sum_{x \in B} r_{\sigma(x)} = \sum_{\lambda \in A'} r_\lambda + r_{\sigma(b)} = \sum_{\lambda \in A} r_\lambda.$$

∎

Lemma 1.19. *If* $\{a_\lambda\}_{\lambda \in A}$ *and* $\{b_\lambda\}_{\lambda \in A}$ *are two sequences in* R, *then*

$$\sum_{\lambda \in A} (a_\lambda + b_\lambda) = \sum_{\lambda \in A} a_\lambda + \sum_{\lambda \in A} b_\lambda.$$

Moreover, if we further assume that R *is a ring, then for all* $r \in R$ *we have the right and left distributive laws;,*

$$r \cdot \sum_{\lambda \in A} a_\lambda = \sum_{\lambda \in A} r \cdot a_\lambda \text{ and}$$

$$\left(\sum_{\lambda \in A} a_\lambda \right) \cdot r = \sum_{\lambda \in A} a_\lambda \cdot r.$$

Proof. This follows by induction. Here is the key step. Suppose that $\alpha \in A$ and $A' := A \setminus \{\alpha\}$, then

$$\begin{aligned} \sum_{\lambda \in A} (a_\lambda + b_\lambda) &= \sum_{\lambda \in A'} (a_\lambda + b_\lambda) + (a_\alpha + b_\alpha) \\ &= \sum_{\lambda \in A'} a_\lambda + \sum_{\lambda \in A'} b_\lambda + (a_\alpha + b_\alpha) \quad \text{(by induction)} \\ &= \left(\sum_{\lambda \in A'} a_\lambda + a_\lambda + \right) \left(\sum_{\lambda \in A'} b_\lambda + b_\alpha \right) \quad \begin{pmatrix} \text{commutativity} \\ \text{and associativity} \end{pmatrix} \\ &= \sum_{\lambda \in A} a_\lambda + \sum_{\lambda \in A} b_\lambda. \end{aligned}$$

The multiplicative assertions follows by induction as well,

$$\begin{aligned} r \cdot \sum_{\lambda \in A} a_\lambda = r \cdot \left(\sum_{\lambda \in A'} a_\lambda + a_\alpha \right) &= r \cdot \left(\sum_{\lambda \in A'} a_\lambda \right) + r \cdot a_\alpha \\ &= \left(\sum_{\lambda \in A'} r \cdot a_\lambda \right) + r \cdot a_\alpha \\ &= \sum_{\lambda \in A} r \cdot a_\lambda. \end{aligned}$$

∎

Lecture 2

Recall that a ring is a set, R, with two binary operations "+" = addition and "$\cdot$"= multiplication, such that $(R,+)$ is an abelian group (with identity element we call 0), $(\cdot)$ is an associative multiplication on R which is left and right distributive over "+." Also recall that if there is a multiplicative identity, $1 \in R$ (so $1a = a1 = a$ for all a), we say R is a ring with identity (unity). Furthermore we write $a - b$ for $a + (-b)$. This shows the importance of distributivity. We now continue with giving more examples of rings.

Example 2.1. Let R denote the continuous functions, $f : \mathbb{R} \to \mathbb{R}$ such that $\lim_{x\to\pm\infty} f(x) = 0$. As usual, let $f+g$ and $f \cdot g$ be pointwise addition and multiplication of functions, i.e.

$$(f+g)(x) = f(x) + g(x) \text{ and } (f \cdot g)(x) = f(x)\, g(x) \text{ for all } x \in \mathbb{R}.$$

Then R is a ring without identity. (If we remove the restrictions on the functions at infinity, R would be a ring with identity, namely $\mathbf{1}(x) \equiv 1$.)

Example 2.2. For any collection of rings $R_1, R_2, \ldots, R_m$, define the direct sum to be

$$R = R_1 \oplus \cdots \oplus R_n = \{(r_1, r_2, \ldots, r_n) : r_i \in R_i \text{ all } i\}$$

the set of all m-tuples where the ith coordinate comes from R_i. R is a ring if we define

$$(r_1, r_2, \ldots, r_m) + (s_1, s_2, \ldots, s_m) = (r_1 s_1, r_2 s_2, \ldots, r_m s_m),$$

and

$$(r_1, r_2, \ldots, r_m) + (s_1, s_2, \ldots, s_m) = (r_1 + s_1, r_2 + s_2, \ldots, r_m + s_m).$$

The identity element 0 is $(0, 0, \ldots, 0)$. (Easy to check)

2.1 Polynomial Ring Examples

Example 2.3 (Polynomial rings). Let $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{Z}$ and let $R[x]$ denote the polynomials in x with coefficients from R. We add and multiply polynomials in the usual way. For example if $f = 3x^2 - 2x + 5$ and $g = 5x^2 + 1$, then

$$\begin{aligned} f + g &= 8x^2 - 2x + 6 \text{ and} \\ fg &= (5x^3 + 1)(3x^2 - 2x + 5) \\ &= 5 - 2x + 3x^2 + 25x^3 - 10x^4 + 15x^5. \end{aligned}$$

One may check (see Theorem 2.4 below) that $R[x]$ with these operations is a commutative ring with identity, $\mathbf{1} = 1$.These rules have been chosen so that $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ and $(f \cdot g)(\alpha) = f(\alpha)\, g(\alpha)$ for all $\alpha \in R$ where

$$f(\alpha) := \sum_{i=0}^{\infty} a_i \alpha^i.$$

Theorem 2.4. *Let R be a ring and $R[x]$ denote the collection of polynomials with the usual addition and multiplication rules of polynomials. Then $R[x]$ is again a ring. To be more precise,*

$$R[x] = \left\{ p = \sum_{i=0}^{\infty} p_i x^i : p_i \in R \text{ with } p_i = 0 \text{ a.a.} \right\},$$

where we say that $p_i = 0$ a.a. (read as almost always) provided that $|\{i : p_i \neq 0\}| < \infty$. If $q := \sum_{i=0}^{\infty} q_i x^i \in R[x]$, then we set,

$$p + q := \sum_{i=0}^{\infty} (p_i + q_i)\, x^i \text{ and} \tag{2.1}$$

$$p \cdot q := \sum_{i=0}^{\infty} \left(\sum_{k+l=i} p_k q_l \right) x^i = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} p_k q_{i-k} \right) x^i. \tag{2.2}$$

Proof. The proof is similar to the matrix group examples. Let me only say a few words about the associativity property of multiplication here, since this is the most complicated property to check. Suppose that $r = \sum_{i=0}^{\infty} r_i x^i$, then

$$\begin{aligned}p\,(qr) &= \sum_{n=0}^{\infty}\left(\sum_{i+j=n} p_i\,(qr)_j\right)x^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{i+j=n} p_i\left(\sum_{k+l=j} q_k r_l\right)\right)x^n \\ &= \sum_{n=0}^{\infty}\left(\sum_{i+k+l=n} p_i q_k r_l\right)x^n.\end{aligned}$$

As similar computation shows,

$$(pq)\,r = \sum_{n=0}^{\infty}\left(\sum_{i+k+l=n} p_i q_k r_l\right)x^n$$

and hence the multiplication rule in Eq. (2.2) is associative. ■

2.2 Subrings and Ideals I

We now define the concept of a subring in a way similar to the concept of subgroup.

Definition 2.5 (Subring). *Let R be a ring. If S is subset of R which is itself a ring under the same operations $+,\cdot$ of R restricted to the set S, then S is called a* ***subring*** *of R.*

Lemma 2.6 (Subring test). *$S\subset R$ is a subring if and only if S is a subgroup of $(R,+)$ and S is closed under multiplication. In more detail, S is a subring of R, iff for all $a,b\in S$, that*

$$a+b\in S,\ \ -a\in S,\ \text{ and } ab\in S.$$

Alternatively we may check that

$$a-b\in S,\ \text{ and } ab\in S \text{ for all } a,b\in S.$$

Put one last way, S is a subring of R if $(S,+)$ is a subgroup of $(R,+)$ which is closed under the multiplication operation, i.e. $S\cdot S\subset S$.

Proof. Either of the conditions, $a+b\in S$, $-a\in S$ or $a-b\in S$ for all $a,b\in S$ implies that $(S,+)$ is a subgroup of $(R,+)$. The condition that $(S,\cdot)$ is a closed shows that "$\cdot$" is well defined on S. This multiplication on S then inherits the associativity and distributivity laws from those on R. ■

Definition 2.7 (Ideals). *Let R be a ring. A (two sided) ideal, I, of R is a subring, $I\subset R$ such that $RI\subset R$ and $IR\subset R$. Alternatively put, $I\subset R$ is an ideal if $(I,+)$ is a subgroup of $(R,+)$ such that $RI\subset R$ and $IR\subset R$. (Notice that every ideal, I, of R is also a subring of R.)*

Example 2.8. Suppose that R is a ring with identity 1 and I is an ideal. If $1\in I$, then $I=R$ since $R=R\cdot 1\subset RI\subset I$.

Example 2.9. Given a ring R, R itself and $\{0\}$ are always ideals of R. $\{0\}$ is the trivial ideal. An ideal (subring) $I\subset R$ for which $I\neq R$ is called a proper ideal (subring).

Example 2.10. If R is a commutative ring and $b\in R$ is any element, then the **principle ideal generated by** b, denoted by $\langle b\rangle$ or Rb, is

$$I=Rb=\{rb: r\in R\}.$$

To see that I is an ideal observer that if $r,s\in R$, then rb and sb are generic elements of I and

$$rb-sb=(r-s)b\in Rb.$$

Therefore I is an additive subgroup of R. Moreover, $(rb)\,s=s\,(rb)=(sr)\,b\in I$ so that $RI=IR\subset I$.

Theorem 2.11. *Suppose that $R=\mathbb{Z}$ or $R=\mathbb{Z}_m$ for some $m\in\mathbb{Z}_+$. Then the subgroups of $(R,+)$ are the same as the subrings of R which are the same as the ideals of R. Moreover, every ideal of R is a principle ideal.*

Proof. If $R=\mathbb{Z}$, then $\langle m\rangle=m\mathbb{Z}$ inside of $\mathbb{Z}$ is the principle ideal generated by m. Since every subring, $S\subset\mathbb{Z}$ is also a subgroup and all subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$ for some $m\in\mathbb{Z}$, it flows that all subgroups of $(\mathbb{Z},+)$ are in fact also principle ideals.

Suppose now that $R=\mathbb{Z}_n$. Then again for any $m\in\mathbb{Z}_n$,

$$\langle m\rangle=\{km: k\in\mathbb{Z}\}=m\mathbb{Z}_n \tag{2.3}$$

is the principle ideal in $\mathbb{Z}_n$ generated by m. Conversely if $S\subset\mathbb{Z}_n$ is a sub-ring, then S is in particular a subgroup of $\mathbb{Z}_n$. From last quarter we know that this implies $S=\langle m\rangle=\langle\gcd(n,m)\rangle$ for some $m\in\mathbb{Z}_n$. Thus every subgroup of $(\mathbb{Z}_n,+)$ is a principle ideal as in Eq. (2.3). ■

Example 2.12. The set,

$$S=\left\{\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}: a,b,d\in\mathbb{R}\right\},$$

is a subring of $M_2(\mathbb{R})$. To check this observe that;

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} - \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} a-a & b-b' \\ 0 & d-d' \end{bmatrix} \in S$$

and

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix} = \begin{bmatrix} a'a & ab'+bd' \\ 0 & dd' \end{bmatrix} \in S.$$

S is not an ideal since,

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix} \notin S \text{ if } a \neq 0.$$

Example 2.13. Consider $\mathbb{Z}_m$ and the subset $U(m)$ the set of units in $\mathbb{Z}_m$. Then $U(m)$ is never a subring of $\mathbb{Z}_m$, because $0 \notin U(m)$.

Example 2.14. The collection of matrices,

$$S = \left\{ \begin{bmatrix} 0 & a \\ b & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\},$$

is not a subring of $M_2(\mathbb{R})$. It is an additive subgroup which is however not closed under matrix multiplication;

$$\begin{bmatrix} 0 & a \\ b & c \end{bmatrix} \begin{bmatrix} 0 & a' \\ b' & c' \end{bmatrix} = \begin{bmatrix} ab' & ac' \\ cb' & ba+cc' \end{bmatrix} \notin S$$

Definition 2.15. *Let R be a ring with identity. We say that $S \subset R$ is a* ***unital subring*** *of R if S is a sub-ring containing 1_R. (Most of the subrings we will consider later will be unital.)*

Example 2.16. Here are some examples of unital sub-rings.

1. S in Example 2.12 is a unital sub-ring of $M_2(\mathbb{R})$.
2. The polynomial functions on $\mathbb{R}$ is a unital sub-ring of the continuous functions on $\mathbb{R}$.
3. $\mathbb{Z}[x]$ is a unital sub-ring of $\mathbb{Q}[x]$ or $\mathbb{R}[x]$ or $\mathbb{C}[x]$.
4. $\mathbb{Z}[i] := \{a + ib : a, b \in \mathbb{Z}\}$ is a unital subring of $\mathbb{C}$.

Example 2.17. Here are a few examples of non-unital sub-rings.

1. $n\mathbb{Z} \subset \mathbb{Z}$ is a non-unital subring of $\mathbb{Z}$ for all $n \neq 0$ since $n\mathbb{Z}$ does not even contain an identity element.
2. If $R = \mathbb{Z}_8$, then every non-trivial proper subring, $S = \langle m \rangle$, of R has no identity. The point is if $k \in \mathbb{Z}_8$ is going to be an identity for some sub-ring of $\mathbb{Z}_8$, then $k^2 = k$. It is now simple to check that $k^2 = k$ in $\mathbb{Z}_8$ iff $k = 0$ or 1 which are not contained in any proper non-trivial sub-ring of $\mathbb{Z}_8$. (See Remark 2.18 below.)
3. Let $R := \mathbb{Z}_6$ and $S = \langle 2 \rangle = \{0, 2, 4\}$ is a sub-ring of $\mathbb{Z}_6$. Moreover, one sees that $1_S = 4$ is the unit in S ($4^2 = 4$ and $4 \cdot 2 = 2$) which is not $1_R = 1$. Thus again, S is not a unital sub-ring of $\mathbb{Z}_6$.
4. The set,
$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\} \subset R = M_2(\mathbb{R}),$$
is a subring of $M_2(\mathbb{R})$ with
$$1_S = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_R$$
and hence is not a unital subring of $M_2(\mathbb{R})$.
5. Let v be a non-zero column vector in $\mathbb{R}^2$ and define,
$$S := \{A \in M_2(\mathbb{R}) : Av = 0\}.$$
Then S is a non-unital subring of $M_2(\mathbb{R})$ which is not an ideal. (You should verify these assertions yourself!)

Remark 2.18. Let $n \in \mathbb{Z}_+$ and $S := \langle m \rangle$ be a sub-ring of $\mathbb{Z}_n$. It is natural to ask, when does S have an identity element. To answer this question, we begin by looking for $m \in \mathbb{Z}_n$ such that $m^2 = m$. Given such a m, we claim that m is an identity for $\langle m \rangle$ since

$$(km)\, m = km^2 = k_1 m \text{ for all } km \in \langle m \rangle.$$

The condition that $m^2 = m$ is equivalent to $m(m-1) = 0$, i.e. $n | m(m-1)$. Thus $\langle m \rangle = \langle \gcd(n, m) \rangle$ is a ring with identity iff $n | m(m-1)$.

Example 2.19. Let us take $m = 6$ in the above remark so that $m(m-1) = 30 = 3 \cdot 2 \cdot 5$. In this case 10, 15 and 30 all divide $m(m-1)$ and therefore 6 is the identity element in $\langle 6 \rangle$ thought of as a subring of either, $\mathbb{Z}_{10}$, or $\mathbb{Z}_{15}$, or $\mathbb{Z}_{30}$. More explicitly 6 is the identity in

$$\begin{aligned} \langle 6 \rangle &= \langle \gcd(6, 10) \rangle = \langle 2 \rangle = \{0, 2, 4, 6, 8\} \subset \mathbb{Z}_{10}, \\ \langle 6 \rangle &= \langle \gcd(6, 15) \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12\} \subset \mathbb{Z}_{15}, \text{ and} \\ \langle 6 \rangle &= \langle \gcd(6, 30) \rangle = \{0, 6, 12, 18, 24\} \subset \mathbb{Z}_{30}. \end{aligned}$$

Example 2.20. On the other hand there is no proper non-trivial subring of $\mathbb{Z}_8$ which contains an identity element. Indeed, if $m \in \mathbb{Z}_8$ and $8 = 2^3 | m(m-1)$, then either $2^3 | m$ if m is even or $2^3 | (m-1)$ if m is odd. In either the only $m \in \mathbb{Z}_8$ with this property is $m = 0$ and $m = 1$. In the first case $\langle 0 \rangle = \{0\}$ is the trivial subring of $\mathbb{Z}_8$ and in the second case $\langle 1 \rangle = \mathbb{Z}_8$ is not proper.

Lecture 3

3.1 Some simple ring facts

The next lemma shows that the distributive laws force 0, 1, and the symbol "$-$" to behave in familiar ways.

Lemma 3.1 (Some basic properties of rings). *Let R be a ring. Then;*

1. $a0 = 0 = 0a$ *for all* $a \in R$.
2. $(-a)b = -(ab) = a(-b)$ *for all* $a, b \in R$
3. $(-a)(-b) = ab$ *for all* $a, b \in R$. *In particular, if R has identity* 1, *then*
$$(-1)(-1) = 1 \text{ and}$$
$$(-1)a = -a \text{ for all } a \in R.$$
(This explains why minus times minus is a plus! It has to be true in any structure with additive inverses and distributivity.)
4. *If* $a, b, c \in R$, *then* $a(b-c) = ab - ac$ *and* $(b-c)a = ba - ca$.

Proof. For all $a, b \in R$;

1. $a0 + 0 = a0 = a(0+0) = a0 + a0$, and hence by cancellation in the abelian group, $(R, +)$, we conclude that , so $0 = a0$. Similarly one shows $0 = 0a$.
2. $(-a)b + ab = (-a+a)b = 0b = 0$, so $(-a)b = -(ab)$. Similarly $a(-b) = -ab$.
3. $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$, where in the last equality we have used the inverting an element in a group twice gives the element back.
4. This last item is simple since,
$$a(b-c) := a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab - ac.$$
Similarly one shows that $(b-c)a = ba - ca$.

■

In proofs above the reader should not be fooled into thinking these things are obvious. The elements involved are not necessarily familiar things like real numbers. For example, in $M_2(\mathbb{R})$ item 2 states, $(-I)A = -(IA) = -A$, i.e.

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \checkmark$$

The following example should help to illustrate the significance of Lemma 3.1.

Example 3.2. Consider $R = \langle 2 \rangle = \{0, 2, 4, 6, 8\} \subset \mathbb{Z}_{10}$. From Example 2.19 we know that $1_R = 6$ which you can check directly as well. So $-1_R = -6 \bmod 10 = 4$. Taking $a = 2$ let us write out the meaning of the identity, $(-1_R) \cdot a = -a$;

$$(-1_R) \cdot a = 4 \cdot 2 = 8 = -a.$$

Let us also work out $(-2)(-4)$ and compare this with $2 \cdot 4 = 8$;

$$(-2)(-4) = 8 \cdot 6 = 48 \bmod 10 = 8.$$

Lastly consider,

$$4 \cdot (8-2) = 4 \cdot 6 = 24 \bmod 10 = 4 \text{ while}$$
$$4 \cdot 8 - 4 \cdot 2 = 2 - 8 = -6 \bmod 10 = 4.$$

3.2 The $R[S]$ subrings I

Here we will construct some more examples of rings which are closely related to polynomial rings. In these examples, we will be given a commutative ring R (usually commutative) and a set S equipped with some sort of multiplication, we then are going to define $R[S]$ to be the collection of linear combinations of elements from the set, $\cup_{n=0}^{\infty} RS^n$. Here RS^n consists of formal symbols of the form $rs_1 \dots s_n$ with $r \in R$ and $s_i \in S$. The next proposition gives a typical example of what we have in mind.

A typical case will be where $S = \{s_1, \dots, s_n\}$ is a finite set then

Proposition 3.3. *If $R \subset \bar{R}$ is a sub-ring of a commutative ring $\bar{R}$ and $S = \{s_1, \dots, s_n\} \subset \bar{R}$. Let*

$$R[S] = R[s_1, \dots, s_n] = \left\{ \sum_k a_k s^k : a_k \in R \text{ with } a_k = 0 \text{ a.a.} \right\},$$

where $k = (k_1, \dots k_n) \in \mathbb{N}^n$ and $s^k = s_1^{k_1} \dots s_n^{k_n}$ with $a_0 s^0 := a_0 \in R$. Then $R[s_1, \dots, s_n]$ is a sub-ring of $\bar{R}$.

Proof. If $f=\sum_k a_k s^k$ and $g=\sum_k b_k s^k$, then

$$\begin{aligned} f+g &= \sum_k (a_k+b_k)\, s^k \in R[S], \\ -g &= \sum_k -b_k s^k \in R[S], \text{ and} \\ f\cdot g &= \sum_k a_k s^k \cdot \sum_l b_l s^l \\ &= \sum_{k,l} a_k b_l s^k s^l = \sum_{k,l} a_k b_l s^{k+l} \\ &= \sum_n \left(\sum_{k+l=n} a_k b_l\right) s^n \in R[S]. \end{aligned}$$

■

Example 3.4 (Gaussian Integers). Let $i := \sqrt{-1} \in \mathbb{C}$. Then $\mathbb{Z}[i] = \{x+yi : x,y\in\mathbb{Z}\}$. To see this notice that $i^2=-1\in\mathbb{Z}$, and therefore

$$\begin{aligned} \sum_{k=0}^{\infty} a_k (i)^k &= \sum_{l=0}^{\infty}\left[a_{4l}(i)^{4l} + a_{4l+1}(i)^{4l+1} + a_{4l+2}(i)^{4l+2} + a_{4l+3}(i)^{4l+3}\right] \\ &= \sum_{l=0}^{\infty}\left[a_{4l} + a_{4l+1} i - a_{4l+2} - a_{4l+3} i\right] \\ &= \sum_{l=0}^{\infty}\left[a_{4l}-a_{4l+2}\right] + \left(\sum_{l=0}^{\infty}\left[a_{4l+1}-a_{4l+3}\right]\right) i \\ &= x+yi \end{aligned}$$

where

$$x=\sum_{l=0}^{\infty}\left[a_{4l}-a_{4l+2}\right] \text{ and } y=\sum_{l=0}^{\infty}\left[a_{4l+1}-a_{4l+3}\right].$$

Example 3.5. Working as in the last example we see that

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2} : a,b\in\mathbb{Z}\right\}$$

is a sub-ring of $\mathbb{R}$.

Example 3.6 (Gaussian Integers mod m*).* For any $m\ge 2$, let

$$\mathbb{Z}_m[i] = \{x+yi : x,y\in\mathbb{Z}_m\}$$

with the obvious addition rule and multiplication given by

$$(x+yi)(u+vi) = ux - vy + (uy+vx)\, i \text{ in } \mathbb{Z}_m.$$

The next proposition shows that this is a commutative ring with identity, 1.

Proposition 3.7. *Let R be a commutative ring with identity and let*

$$R[i] := \{a+bi : a,b\in R\} \cong \{(a,b) : a,b\in R\} = R^2.$$

Define addition and multiplication of $R[i]$ as one expects by,

$$(a+bi)+(c+di) = (a+c)+(b+d)\, i$$

and

$$(a+bi)\cdot(c+di) = (ac-bd)+(bc+ad)\, i.$$

Then $(R[i],+,\cdot)$ is a commutative ring with identity.

Proof. This can be checked by brute force. Rather than use brute force lets give a proof modeled on Example 1.11, i.e. we will observe that we may identify $R[i]$ with a unital subring of $M_2(R)$. To do this we take,

$$\mathbf{i} := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in M_2(R) \text{ and } 1 := I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2(R).$$

Thus we take,

$$a+ib \longleftrightarrow aI + b\mathbf{i} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in M_2(R).$$

Since

$$\begin{aligned} (aI+b\mathbf{i})+(cI+d\mathbf{i}) &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix} \\ &= (a+c)\, I + (b+d)\, \mathbf{i} \end{aligned}$$

and

$$\begin{aligned} (aI+b\mathbf{i})(cI+d\mathbf{i}) &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix}\begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix} \\ &= (ac-bd)\, I + (bc+ad)\, \mathbf{i} \end{aligned}$$

we see that

$$S := \left\{\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = aI + b\mathbf{i} : a,b\in R\right\}$$

is indeed a unital sub-ring of $M_2(R)$. Moreover, the multiplication rules on S and $R[i]$ agree under the identification; $a+ib \longleftrightarrow aI+b\mathbf{i}$. Therefore we may conclude that $(R[i],+,\cdot)$ satisfies the properties of a ring. ■

3.3 Appendix: $R[S]$ rings II

You may skip this section on first reading.

Definition 3.8. *Suppose that S is a set which is equipped with an associative binary operation, $\cdot$, which has a unique unit denoted by e. (We do not assume that $(S,\cdot)$ has inverses. Also suppose that R is a ring, then we let $R[S]$ consist of the formal sums, $\sum_{s\in S} a_s s$ where $\{a_s\}_{s\in S} \subset R$ is a sequence with finite support, i.e. $|\{s\in S : a_s \neq 0\}| < \infty$. We define two binary operations on $R[S]$ by,*

$$\sum_{s\in S} a_s s + \sum_{s\in S} b_s s := \sum_{s\in S} (a_s + b_s) s$$

and

$$\begin{aligned}\sum_{s\in S} a_s s \cdot \sum_{s\in S} b_s s &= \sum_{s\in S} a_s s \cdot \sum_{t\in S} b_t t \\ &= \sum_{s,t\in S} a_s b_t st = \sum_{u\in S}\left(\sum_{st=u} a_s b_t\right) u.\end{aligned}$$

So really we $R[S]$ are those sequences $a := \{a_s\}_{s\in S}$ with finite support with the operations,

$$(a+b)_s = a_s + b_s \text{ and } (a\cdot b)_s = \sum_{uv=s} a_u b_v \text{ for all } s \in S.$$

Theorem 3.9. *The set $R[S]$ equipped with the two binary operations $(+,\cdot)$ is a ring.*

Proof. Because $(R,+)$ is an abelian group it is easy to check that $(R[S],+)$ is an abelian group as well. Let us now check that $\cdot$ is associative on $R[S]$. To this end, let $a,b,c \in R[S]$, then

$$\begin{aligned}[a(bc)]_s &= \sum_{uv=s} a_u (bc)_v = \sum_{uv=s} a_u \left(\sum_{\alpha\beta=v} b_\alpha c_\beta\right) \\ &= \sum_{u\alpha\beta=s} a_u b_\alpha c_\beta\end{aligned}$$

while

$$\begin{aligned}[(ab)c]_s &= \sum_{\alpha\beta=s} (ab)_\alpha c_\beta = \sum_{\alpha\beta=s}\sum_{uv=\alpha} a_u b_v c_\beta \\ &= \sum_{uv\beta=s} a_u b_v c_\beta = \sum_{u\alpha\beta=s} a_u b_\alpha c_\beta = [a(bc)]_s\end{aligned}$$

as desired. Secondly,

$$\begin{aligned}[a\cdot(b+c)]_s &= \sum_{uv=s} a_u (b+c)_v = \sum_{uv=s} a_u (b_v + c_v) \\ &= \sum_{uv=s} a_u b_v + \sum_{uv=s} a_u c_v \\ &= [a\cdot b]_s + [a\cdot c]_s = [a\cdot b + a\cdot c]_s\end{aligned}$$

from which it follows that $a\cdot(b+c) = a\cdot b + a\cdot c$. Similarly one shows that $(b+c)\cdot a = b\cdot a + c\cdot a$.

Lastly if S has an identity, e, and $\mathbf{e}_s := 1_{s=e} \in R$, then

$$[a\cdot \mathbf{e}]_s = \sum_{uv=s} a_u \mathbf{e}_v = a_s$$

from which it follows that $\mathbf{e}$ is the identity in $R[S]$. ∎

Example 3.10 (Polynomial rings). Let x be a formal symbol and let $S := \{x^k : k = 0,1,2\dots\}$ with $x^k x^l := x^{k+l}$ being the binary operation of S. Notice that x^0 is the identity in S under this multiplication rule. Then for any ring R, we have

$$R[S] = \left\{p(x) := \sum_{k=0}^{n} p_k x^k : p_k \in R \text{ and } n \in \mathbb{N}\right\}.$$

The multiplication rule is given by

$$p(x)\,q(x) = \sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} p_j q_{k-j}\right) x^k$$

which is the usual formula for multiplication of polynomials. In this case it is customary to write $R[x]$ rather than $R[S]$.

This example has natural generalization to multiple indeterminants as follows.

Example 3.11. Suppose that $x = (x_1,\dots,x_d)$ are d indeterminants and $k = (k_1,\dots,k_d)$ are multi-indices. Then we let

$$S := \left\{x^k := x_1^{k_1}\dots x_d^{k_d} : k \in \mathbb{N}^d\right\}$$

with multiplication law given by

$$x^k x^{k'} := x^{k+k'}.$$

Then

$$R[S] = \left\{ p(x) := \sum_k p_k x^k : p_k \in R \text{ with } p_k = 0 \text{ a.a.} \right\}.$$

We again have the multiplication rule,

$$p(x)\, q(x) = \sum_k \left(\sum_{j \le k} p_j q_{k-j} \right) x^k.$$

As in the previous example, it is customary to write $R[x_1, \dots, x_d]$ for $R[S]$.

In the next example we wee that the multiplication operation on S need not be commutative.

Example 3.12 (Group Rings). In this example we take $S = G$ where G is a group which need not be commutative. Let R be a ring and set,

$$R[G] := \{a : G \to R| \ |\{g :\in G\} : a(g) \ne 0| < \infty\}.$$

We will identify $a \in R[G]$ with the formal sum,

$$a := \sum_{g \in G} a(g)\, g.$$

We define $(a+b)(g) := a(g) + b(g)$ and

$$\begin{aligned} a \cdot b &= \left(\sum_{g \in G} a(g)\, g \right) \left(\sum_{k \in G} b(k)\, k \right) = \sum_{g,k \in G} a(g)\, b(k)\, gk \\ &= \sum_{h \in G} \left(\sum_{gk = h} a(g)\, b(k) \right) h = \sum_{h \in G} \left(\sum_{g \in G} a(g)\, b\left(g^{-1}h\right) \right) h. \end{aligned}$$

So formally we define,

$$\begin{aligned} (a \cdot b)(h) &:= \sum_{g \in G} a(g)\, b\left(g^{-1}h\right) = \sum_{g \in G} a(hg)\, b\left(g^{-1}\right) = \sum_{g \in G} a\left(hg^{-1}\right) b(g) \\ &= \sum_{gk = h} a(g)\, b(k). \end{aligned}$$

We now claim that R is a ring which is non − commutative when G is non-abelian.

Let us check associativity and distributivity of $\cdot$. To this end,

$$\begin{aligned} [(a \cdot b) \cdot c](h) &= \sum_{gk = h} (a \cdot b)(g) \cdot c(k) \\ &= \sum_{gk = h} \left[\sum_{uv = g} a(u) \cdot b(v) \right] \cdot c(k) \\ &= \sum_{uvk = h} a(u) \cdot b(v) \cdot c(k) \end{aligned}$$

while on the other hand,

$$\begin{aligned} [a \cdot (b \cdot c)](h) &= \sum_{uy = h} a(u) \cdot (b \cdot c)(y) \\ &= \sum_{uy = h} a(u) \cdot \left(\sum_{vk = y} b(v) \cdot c(y) \right) \\ &= \sum_{uvk = h} a(u) \cdot (b(v) \cdot c(y)) \\ &= \sum_{uvk = h} a(u) \cdot b(v) \cdot c(k). \end{aligned}$$

For distributivity we find,

$$\begin{aligned} [(a+b) \cdot c](h) &= \sum_{gk = h} (a+b)(g) \cdot c(k) = \sum_{gk = h} (a(g) + b(g)) \cdot c(k) \\ &= \sum_{gk = h} (a(g) \cdot c(k) + b(g) \cdot c(k)) \\ &= \sum_{gk = h} a(g) \cdot c(k) + \sum_{gk = h} b(g) \cdot c(k) \\ &= [a \cdot c + b \cdot c](h) \end{aligned}$$

with a similar computation showing $c \cdot (a+b) = c \cdot a + c \cdot b$.

Lecture 4

4.1 Units

Definition 4.1. *Suppose R is a ring with identity. A* ***unit*** *of a ring is an element $a \in R$ such that there exists an element $b \in R$ with $ab = ba = 1$. We let $U(R) \subset R$ denote the units of R.*

Notice that in fact $a = b$ in this definition since,

$$a = a \cdot 1 = a(ub) = (au)b = 1 \cdot b = b.$$

Moreover this argument shows that a satisfying $au = 1 = ua$ is unique if it exists. For this reason we will write u^{-1} for a.

Proposition 4.2. *The set $U(R)$ equipped the multiplication law of R is a group.*

Proof. This is a straight forward verification – see the homework assignment. The main point is to observe that $u, v \in U(R)$, then $a := v^{-1}u^{-1}$ satisfies, $a(uv) = 1 = (uv)a$, showing $U(R)$ is closed under the multiplication operation of R. ∎

Example 4.3. In $M_2(\mathbb{R})$, the units in this ring are exactly the elements in $GL(2, \mathbb{R})$, i.e.

$$U(M_2(\mathbb{R})) = GL(2, \mathbb{R}) = \{A \in M_2(\mathbb{R}) : \det A \neq 0\}.$$

If you look back at last quarters notes you will see that we have already proved the following theorem. I will repeat the proof here for completeness.

Theorem 4.4 ($U(\mathbb{Z}_m) = U(m)$). *For any $m \geq 2$,*

$$U(\mathbb{Z}_m) = U(m) = \{a \in \{1, 2, \dots, m-1\} : \gcd(a, m) = 1\}.$$

Proof. If $a \in U(\mathbb{Z}_m)$, there there exists $r \in \mathbb{Z}_m$ such that $1 = r \cdot a = ra \bmod m$. Equivalently put, $m | (ra - 1)$, i.e. there exists t such that $ra - 1 = tm$. Since $1 = ra - tm$ it follows that $\gcd(a, m) = 1$, i.e. that $a \in U(m)$.

Conversely, if $a \in U(m) \iff \gcd(a, m) = 1$ which we know implies there exists $s, t \in \mathbb{Z}$ such that $sa + tm = 1$. Taking this equation $\bmod m$ and letting $b := s \bmod m \in \mathbb{Z}_m$, we learn that $b \cdot a = 1$ in $\mathbb{Z}_m$, i.e. $a \in U(\mathbb{Z}_m)$. ∎

Example 4.5. In $\mathbb{R}$, the units are exactly the elements in $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ that is $U(\mathbb{R}) = \mathbb{R}^\times$.

Example 4.6. Let R be the non-commutative ring of linear maps from $\mathbb{R}^\infty$ to $\mathbb{R}^\infty$ where

$$\mathbb{R}^\infty = \{(a_1, a_2, a_3, \dots) : a_i \in \mathbb{R} \text{ for all } i\},$$

which is a vector space over $\mathbb{R}$. Further let $A, B \in R$ be defined by

$$A(a_1, a_2, a_3, \dots) = (0, a_1, a_2, a_3, \dots) \text{ and}$$
$$B(a_1, a_2, a_3, \dots) = (a_2, a_3, a_4, \dots).$$

Then $BA = \mathbf{1}$ where

$$\mathbf{1}(a_1, a_2, a_3, \dots) = (a_1, a_2, a_3, \dots)$$

while

$$AB(a_1, a_2, a_3, \dots) = (0, a_2, a_3, \dots) \neq \mathbf{1}(a_1, a_2, a_3, \dots).$$

This shows that even though $BA = \mathbf{1}$ it is not necessarily true that $AB = 1$. Neither A nor B are units of $\mathbb{R}^\infty$.

4.2 (Zero) Divisors and Integral Domains

Definition 4.7 (Divisors). *Let R be a ring. We say that for elements $a, b \in R$ that a* ***divides*** *b if there exists an element c such that $ac = b$.*

Note that if $R = \mathbb{Z}$ then this is the usual notion of whether one integer evenly divides another, e.g., 2 divides 6 and 2 doesn't divide 5.

Definition 4.8 (Zero divisors). *A nonzero element $a \in R$ is called a* ***zero divisor*** *if there exists another nonzero element $b \in R$ such that $ab = 0$, i.e. a divides 0 in a nontrivial way. (The trivial way for $a|0$ is; $0 = a \cdot 0$ as this always holds.)*

Definition 4.9 (Integral domain). *A commutative ring R with no zero divisors is called an* ***integral domain*** *(or just a* ***domain****). Alternatively put, R should satisfy, $ab \neq 0$ for all $a, b \in R$ with $a \neq 0 \neq b$.*

Example 4.10. The most familiar rings to you, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have no zero-divisors and hence are integral domains.. In these number systems, it is a familiar fact that $ab = 0$ implies either $a = 0$ or $b = 0$. Another integral domain is the polynomial ring $\mathbb{R}[x]$, see Proposition 4.13 below.

Example 4.11. The ring, $\mathbb{Z}_6$, is not an integral domain. For example, $2 \cdot 3 = 0$ with $2 \neq 0 \neq 3$, so both 2 and 3 are zero divisors.

Lemma 4.12. *The ring $\mathbb{Z}_m$ is an integral domain iff m is prime.*

Proof. If m is prime we know that $U(\mathbb{Z}_m) = U(m) = \mathbb{Z}_m \setminus \{0\}$. Therefore if $a, b \in \mathbb{Z}_m$ with $a \neq 0$ and $ab = 0$ then $b = a^{-1}ab = a^{-1}0 = 0$.

If $m = a \cdot b$ with $a, b \in \mathbb{Z}_m \setminus \{0\}$, then $ab = 0$ while both a and b are not equal to zero in $\mathbb{Z}_m$. ■

Proposition 4.13. *If R is an integral domain, then so is $R[x]$. Conversely if R is not an integral domain then neither is $R[x]$.*

Proof. If $f, g \in R[x]$ are two non-zero polynomials. Then $f = a_n x^n +$ l.o.ts. (lower order terms) and $g = b_m x^m +$ l.o.ts. with $a_n \neq 0 \neq b_m$ and therefore,

$$fg = a_n b_m x^{n+m} + \text{l.o.ts.} \neq 0 \text{ since } a_n b_m \neq 0.$$

The proof of the second assertion is left to the reader. ■

Example 4.14. All of the following rings are integral domains; $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$. We also know that $\mathbb{Z}_m[x]$ is an integral domain iff m is prime.

Example 4.15. If R is the direct product of at least 2 rings, then R has zero divisors. For example if $R = \mathbb{Z} \oplus \mathbb{Z}$, then $(0, b)(a, 0) = (0, 0)$ for all $a, b \in \mathbb{Z}$.

Example 4.16. If R is an integral domain, then any unital subring $S \subset R$ is also an integral domain. In particular, for any $\theta \in \mathbb{C}$, then $\mathbb{Z}[\theta]$, $\mathbb{Q}[\theta]$, and $\mathbb{R}[\theta]$ are all integral domains.

Remark 4.17. It is not true that if R is not an integral domain then every subring, $S \subset R$ is also not an integral domain. For an example, take $R := \mathbb{Z} \oplus \mathbb{Z}$ and $S := \{(a, a) : a \in \mathbb{Z}\} \subset R$. (In the language of Section 5.1 below, $S = \{n \cdot (1, 1) : n \in \mathbb{Z}\}$ which is the sub-ring generated by $1 = (1, 1)$. Similar to this counter example, commutative ring with identity which is not an integral domain but has characteristic being either 0 or prime would give a counter example.)

Domains behave more nicely than arbitrary rings and for a lot of the quarter we will concentrate exclusively on domains. But in a lot of ring theory it is very important to consider rings that are not necessarily domains like matrix rings.

Theorem 4.18 (Cancellation). *If R is an integral domain and $ab = ac$ with $a \neq 0$, then $b = c$. Conversely if R is a commutative ring with identity satisfying this cancellation property then R has no zero divisors and hence is an integral domain.*

Proof. If $ab = ac$, then $a(b - c) = 0$. Hence if $a \neq 0$ and R is an integral domain, then $b - c = 0$, i.e. $b = c$.

Conversely, if R satisfies cancellation and $ab = 0$. If $a \neq 0$, then $ab = a \cdot 0$ and so by cancellation, $b = 0$. This shows that R has no zero divisors. ■

Example 4.19. The ring, $M_2(\mathbb{R})$ contains many zero divisors. For example

$$\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

So in $M_2(\mathbb{R})$ we can not conclude that $B = 0$ if $AB = 0$ with $A \neq 0$, i.e. cancellation does not hold.

4.3 Fields

If we add one more restriction to a domain we get a familiar class of objects called fields.

Definition 4.20 (Fields). *A ring R is a **field** if R is a commutative ring with identity and $U(R) = R \setminus \{0\}$, that is, every non-zero element of R is a unit, in other words has a multiplicative inverse.*

Lemma 4.21 (Fields are domains). *If R is a field then R is an integral domain.*

Proof. If R is a field and $xy = 0$ in R for some x, y with $x \neq 0$, then

$$0 = x^{-1}0 = x^{-1}xy = y.$$

■

Example 4.22. $\mathbb{Z}$ is an integral domain that is not a field. For example $2 \neq 0$ has no multiplicative inverse. The inverse to 2 should be $\frac{1}{2}$ which exists in $\mathbb{Q}$ but not in $\mathbb{Z}$. On the other hand, $\mathbb{Q}$ and $\mathbb{R}$ are fields as the non-zero elements have inverses back in $\mathbb{Q}$ and $\mathbb{R}$ respectively.

Example 4.23. We have already seen that $\mathbb{Z}_m$ is a field iff m is prime. This follows directly form the fact that $U(\mathbb{Z}_m) = U(m)$ and $U(m) = \mathbb{Z}_m \setminus \{0\}$ iff m is prime. Recall that we also seen that $\mathbb{Z}_m$ is an integral domain iff m is prime so it follows $\mathbb{Z}_m$ is a field iff it is an integral domain iff m is prime. When p is prime, we will often denote $\mathbb{Z}_p$ by $\mathbb{F}_p$ to indicate that we are viewing $\mathbb{Z}_p$ is a field.

Lecture 5

In fact, there is another way we could have seen that $\mathbb{Z}_p$ is a field, using the following useful lemma.

Lemma 5.1. *If R be an integral domain with finitely many elements, then R is a field.*

Proof. Let $a \in R$ with $a \neq 0$. We need to find a multiplicative inverse for a. Consider $a, a^2, a^3, \ldots$. Since R is finite, the elements on this list are not all distinct. Suppose then that $a^i = a^j$ for some $i > j \geq 1$. Then $a^j a^{i-j} = a^j \cdot 1$. By cancellation, since R is a domain, $a^{i-j} = 1$. Then a^{i-j-1} is the inverse for a. Note that $a^{i-j-1} \in R$ makes sense because $i - j - 1 \geq 0$. ■

For general rings, a^n only makes sense for $n \geq 1$. If $1 \in R$ and $a \in U(R)$, we may define $a^0 = 1$ and $a^{-n} = \left(a^{-1}\right)^n$ for $n \in \mathbb{Z}_+$. As for groups we then have $a^n a^m = a^{n+m}$ for all $m, n \in \mathbb{Z}$. makes sense for all $n \in \mathbb{Z}$, but in generally negative powers don't always make sense in a ring. Here is another very interesting example of a field, different from the other examples we've written down so far.

Example 5.2. Lets check that $\mathbb{C}$ is a field. Given $0 \neq a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$, $i = \sqrt{-1}$, we need to find $(a + ib)^{-1} \in \mathbb{C}$. Working formally; we expect,

$$\begin{aligned}(a+ib)^{-1} &= \frac{1}{a+bi} = \frac{1}{a+bi}\frac{a-bi}{a-bi}\frac{a-bi}{a^2+b^2} \\ &= \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{C},\end{aligned}$$

which makes sense if $N(a+ib) := a^2 + b^2 \neq 0$, i.e. $a + ib \neq 0$. A simple direct check show that this formula indeed gives an inverse to $a + ib$;

$$\begin{aligned}&(a+ib)\left[\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right] \\ &\quad = \frac{1}{a^2+b^2}(a+ib)(a-ib) = \frac{1}{a^2+b^2}\left(a^2+b^2\right) = 1.\end{aligned}$$

So if $a + ib \neq 0$ we have shown

$$(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Example 5.3. I claim that $R := \mathbb{Z}_3[i] = \mathbb{Z}_3 + i\mathbb{Z}_3$ is a field where we use the multiplication rule,

$$(a+ib)(c+id) = (ac - bd) + i(bc + ad).$$

The main point to showing this is a field beyond showing R is a ring (see Proposition 3.7) is to show $(a+ib)^{-1}$ exists in R whenever $a + ib \neq 0$. Working formally for the moment we should have,

$$\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}.$$

This suggest that

$$(a+ib)^{-1} = \left(a^2+b^2\right)^{-1}(a-ib).$$

In order for the latter expression to make sense we need to know that $a^2 + b^2 \neq 0$ in $\mathbb{Z}_3$ if $(a,b) \neq 0$ which we can check by brute force;

a	0	0	0	1	1	1	2	2	2
b	0	1	2	0	1	2	0	1	2
$N(a+ib) = a^2+b^2$	0	1	1	1	2	2	1	2	2

.

Alternatively we may show $\mathbb{Z}_3[i]$ is an integral domain and then use Lemma 5.1. Notice that

$$\begin{aligned}&(a+ib)(c+id) = 0 \implies (a-ib)(a+ib)(c+id) = 0 \text{ i.e.} \\ &\left(a^2+b^2\right)(c+id) = 0.\end{aligned}$$

So using the chart above, we see that $a^2 + b^2 = 0$ iff $a + ib = 0$ and therefore, if $a + ib \neq 0$ then $c + id = 0$.

5.1 Characteristic of a Ring

Notation 5.4 *Suppose that $a \in R$ where R is a ring. Then for $n \in \mathbb{Z}$ we define $n \cdot a \in R$ by, $0_{\mathbb{Z}} \cdot a = 0_R$ and*

$$n \cdot a = \begin{cases} \overbrace{a + \cdots + a}^{n \text{ times}} & \text{if } n \geq 1 \\ -\overbrace{(a + \cdots + a)}^{|n| \text{ times}} = |n| \cdot (-a) & \text{if } n \leq -1 \end{cases}.$$

So $3 \cdot a = a + a + a$ *while* $-2 \cdot a = -a - a$.

Lemma 5.5. *Suppose that* R *is a ring and* $a, b \in R$. *Then for all* $m, n \in \mathbb{Z}$ *we have*

$$(m \cdot a)\, b = m \cdot (ab)\,, \tag{5.1}$$
$$a\,(m \cdot b) = m \cdot (ab)\,. \tag{5.2}$$

We also have

$$-(m \cdot a) = (-m) \cdot a = m \cdot (-a) \text{ and} \tag{5.3}$$
$$m \cdot (n \cdot a) = mn \cdot a. \tag{5.4}$$

Proof. If $m = 0$ both sides of Eq. (5.1) are zero. If $m \in \mathbb{Z}_+$, then using the distributive associativity laws repeatedly gives;

$$\begin{aligned} (m \cdot a)\, b &= \overbrace{(a + \cdots + a)}^{m \text{ times}} b \\ &= \overbrace{(ab + \cdots + ab)}^{m \text{ times}} = m \cdot (ab)\,. \end{aligned}$$

If $m < 0$, then

$$(m \cdot a)\, b = (|m| \cdot (-a))\, b = |m| \cdot ((-a)\, b) = |m| \cdot (-ab) = m \cdot (ab)$$

which completes the proof of Eq. (5.1). The proof of Eq. (5.2) is similar and will be omitted.

If $m = 0$ Eq. (5.3) holds. If $m \geq 1$, then

$$-(m \cdot a) = -\overbrace{(a + \cdots + a)}^{m \text{ times}} = \overbrace{((-a) + \cdots + (-a))}^{m \text{ times}} = m \cdot (-a) = (-m) \cdot a.$$

If $m < 0$, then

$$-(m \cdot a) = -(|m| \cdot (-a)) = (-|m|) \cdot (-a) = m \cdot (-a)$$

and

$$-(m \cdot a) = -(|m| \cdot (-a)) = (|m| \cdot (-(-a))) = |m| \cdot a = (-m) \cdot a.$$

which proves Eq. (5.3).

Letting $x := \operatorname{sgn}(m)\operatorname{sgn}(n)a$, we have

$$\begin{aligned} m \cdot (n \cdot a) = |m| \cdot (|n| \cdot x) &= \overbrace{(|n| \cdot x + \cdots + |n| \cdot x)}^{|m| \text{ times}} \\ &= \overbrace{\overbrace{(x + \cdots + x)}^{|n| \text{ times}} + \cdots + \overbrace{(x + \cdots + x)}^{|n| \text{ times}}}^{|m| \text{ times}} \\ &= (|m|\, |n|) \cdot x = mn \cdot a. \end{aligned}$$

■

Corollary 5.6. *If* R *is a ring,* $a, b \in R$, *and* $m, n \in \mathbb{Z}$, *then*

$$(m \cdot a)\,(n \cdot b) = mn \cdot ab. \tag{5.5}$$

Proof. Using Lemma 5.5 gives;

$$(m \cdot a)\,(n \cdot b) = m \cdot (a\,(n \cdot b)) = m \cdot (n \cdot (ab)) = mn \cdot ab.$$

■

Corollary 5.7. *Suppose that* R *is a ring and* $a \in R$. *Then for all* $m, n \in \mathbb{Z}$,

$$(m \cdot a)\,(n \cdot a) = mn \cdot a^2.$$

In particular if $a = 1 \in R$ *we have,*

$$(m \cdot 1)\,(n \cdot 1) = mn \cdot 1.$$

Unlike the book, we will only bother to define the characteristic for rings which have an identity, $1 \in R$.

Definition 5.8 (Characteristic of a ring). *Let* R *be a ring with* $1 \in R$. *The characteristic,* $\operatorname{chr}(R)$, *of* R *is is the order of the element* 1 *in the additive group* $(R, +)$. *Thus* n *is the smallest number in* $\mathbb{Z}_+$ *such that* $n \cdot 1 = 0$. *If no such* $n \in \mathbb{Z}_+$ *exists, we say that characteristic of* R *is* 0 *by convention and write* $\operatorname{chr}(R) = 0$.

Lemma 5.9. *If* R *is a ring with identity and* $\operatorname{chr}(R) = n \geq 1$, *then* $n \cdot x = 0$ *for all* $x \in R$.

Proof. For any $x \in R$, $n \cdot x = n \cdot (1x) = (n \cdot 1)\, x = 0x = 0$. ■

Lemma 5.10. *Let* R *be a domain. If* $n = \operatorname{chr}(R) \geq 1$, *then* n *is a prime number.*

Proof. If n is not prime, say $n = pq$ with $1 < p < n$ and $1 < q < n$, then

$$(p \cdot 1_R)(q \cdot 1_R) = pq \cdot (1_R 1_R) = pq \cdot 1_R = n \cdot 1_R = 0.$$

As $p \cdot 1_R \neq 0$ and $q \cdot 1_R \neq 0$ and we may conclude that both $p \cdot 1_R$ and $q \cdot 1_R$ are zero divisors contradicting the assumption that R is an integral domain. ∎

Example 5.11. The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}\left[\sqrt{d}\right] := \mathbb{Q} + \mathbb{Q}\sqrt{d}$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{Z}[x]$ all have characteristic 0.

For each $m \in \mathbb{Z}_+$, $\mathbb{Z}_m$ and $\mathbb{Z}_m[x]$ are rings with characteristic m.

Example 5.12. For each prime, p, $\mathbb{F}_p := \mathbb{Z}_p$ is a field with characteristic p. We also know that $\mathbb{Z}_3[i]$ is a field with characteristic 3. Later, we will see other examples of fields of characteristic p.

Lecture 6

6.1 Square root field extensions of $\mathbb{Q}$

Recall that $\sqrt{2}$ is irrational. Indeed suppose that $\sqrt{2} = m/n \in \mathbb{Q}$ and, with out loss of generality, assume that $\gcd(m,n) = 1$. Then $m^2 = 2n^2$ from which it follows that $2|m^2$ and so $2|m$ by Euclid's lemma. However, it now follows that $2^2|2n^2$ and so $2|n^2$ which again by Euclid's lemma implies $2|n$. However, we assumed that m and n were relatively prime and so we have a contradiction and hence $\sqrt{2}$ is indeed irrational. As a consequence of this fact, we know that $\{1, \sqrt{2}\}$ are linearly independent over $\mathbb{Q}$, i.e. if $a + b\sqrt{2} = 0$ then $a = 0 = b$.

Example 6.1. In this example we will show,

$$R = \mathbb{Q}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \tag{6.1}$$

is a field. Using similar techniques to those in Example 3.4 we see that $\mathbb{Q}\left[\sqrt{2}\right]$ may be described as in Eq. (6.1) and hence is a subring of $\mathbb{Q}$ by Proposition 3.3. Alternatively one may check directly that the right side of Eq. (6.1) is a subring of $\mathbb{Q}$ since;

$$a + b\sqrt{2} - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in R$$

and

$$\begin{aligned}(a + b\sqrt{2})(c + d\sqrt{2}) &= ac + bc\sqrt{2} + ad\sqrt{2} + bd(2) \\ &= (ac + 2bd) + (bc + ad)\sqrt{2} \in R.\end{aligned}$$

So by either means we see that R is a ring and in fact an integral domain by Example 4.16. It does not have finitely many elements so we can't use Lemma 5.1 to show it is a field. However, we can find $\left(a + b\sqrt{2}\right)^{-1}$ directly as follows. If $\xi = \left(a + b\sqrt{2}\right)^{-1}$, then

$$1 = (a + b\sqrt{2})\xi$$

and therefore,

$$a - b\sqrt{2} = (a - b\sqrt{2})(a + b\sqrt{2})\xi = \left(a^2 - 2b^2\right)\xi$$

which implies,

$$\xi = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}\left[\sqrt{2}\right].$$

Moreover, it is easy to check this ξ works provided $a^2 - 2b^2 \neq 0$. But if $a^2 - 2b^2 = 0$ with $b \neq 0$, then $\sqrt{2} = |a| / |b|$ showing $\sqrt{2}$ is irrational which we know to be false – see Proposition 6.2 below for details. Therefore, $\mathbb{Q}\left[\sqrt{2}\right]$ is a field.

Observe that $\mathbb{Q} \subsetneq R := \mathbb{Q}\left[\sqrt{2}\right] \subsetneq \mathbb{R}$. Why is this? One reason is that $R := \mathbb{Q}\left[\sqrt{2}\right]$ is countable and $\mathbb{R}$ is uncountable. Or it is not hard to show that an irrational number selected more or less at random is not in R. For example, you could show that $\sqrt{3} \notin R$. Indeed if $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$ then

$$3 = a^2 + 2ab\sqrt{2} + 2b^2$$

and hence $2ab\sqrt{2} = 3 - a^2 - 2b^2$. Since $\sqrt{2}$ is irrational, this can only happen if either $a = 0$ or $b = 0$. If $b = 0$ we will have $\sqrt{3} \in \mathbb{Q}$ which is false and if $a = 0$ we will have $3 = 2b^2$. Writing $b = \frac{k}{l}$, this with $\gcd(k, l) = 1$, we find $3l^2 = 2k^2$ and therefore $2|l$ by Gauss' lemma. Hence $2^2|2k^2$ which implies $2|k$ and therefore $\gcd(k, l) \geq 2 > 1$ which is a contradiction. Hence it follows that $\sqrt{3} \neq a + b\sqrt{2}$ for any $a, b \in \mathbb{Q}$.

The following proposition is a natural extension of Example 6.1.

Proposition 6.2. *For all $d \in \mathbb{Z} \setminus \{0\}$, $F := \mathbb{Q}\left[\sqrt{d}\right]$ is a field. (As we will see in the proof, we need only consider those d which are "square prime" free.*

Proof. As $F := \mathbb{Q}\left[\sqrt{d}\right] = \mathbb{Q} + \mathbb{Q}\sqrt{d}$ is a subring of $\mathbb{R}$ which is an integral domain, we know that F is again an integral domain. Let $d = \varepsilon p_1^{k_1} \dots p_n^{k_n}$ with $\varepsilon \in \{\pm 1\}$, $p_1, \dots, p_n$ being distinct primes, and $k_i \geq 1$. Further let $\delta = \varepsilon \prod_{i:k_i \text{ is odd}} p_i$, then $\sqrt{d} = m\sqrt{\delta}$ for some integer m and therefore it easily follows that $F = \mathbb{Q}\left[\sqrt{\delta}\right]$. So let us now write $\delta = \varepsilon p_1 \dots p_k$ with $\varepsilon \in \{\pm 1\}$, $p_1, \dots, p_k$ being distinct primes so that δ is **square prime free.**

Working as above we look for the inverse to $a + b\sqrt{\delta}$ when $(a, b) \neq 0$. Thus we will look for $u, v \in \mathbb{Q}$ such that

$$1 = \left(a + b\sqrt{\delta}\right)\left(u + v\sqrt{\delta}\right).$$

Multiplying this equation through by $a - b\sqrt{\delta}$ shows,

$$a - b\sqrt{\delta} = \left(a^2 - b^2\delta\right)\left(u + v\sqrt{\delta}\right)$$

so that

$$u + v\sqrt{\delta} = \frac{a}{a^2 - b^2\delta} - \frac{b}{a^2 - b^2\delta}\sqrt{\delta}. \tag{6.2}$$

Thus we may define,

$$\left(a + b\sqrt{\delta}\right)^{-1} = \frac{a}{a^2 - b^2\delta} - \frac{b}{a^2 - b^2\delta}\sqrt{\delta}$$

provided $a^2 - b^2\delta \neq 0$ when $(a, b) \neq (0, 0)$.

Case 1. If $\delta < 0$ then $a^2 - b^2\delta = a^2 + |\delta| b^2 = 0$ iff $a = 0 = b$.

Case 2. If $\delta \geq 2$ and suppose that $a, b \in \mathbb{Q}$ with $a^2 = b^2\delta$. For sake of contradiction suppose that $b \neq 0$. By multiplying $a^2 = b^2\delta$ though by the denominators of a^2 and b^2 we learn there are integers, $m, n \in \mathbb{Z}_+$ such that $m^2 = n^2\delta$. By replacing m and n by $\frac{m}{\gcd(m,n)}$ and $\frac{n}{\gcd(m,n)}$, we may assume that m and n are relatively prime.

We now have $p_1 | \left(n^2\delta\right)$ implies $p_1 | m^2$ which by Euclid's lemma implies that $p_1 | m$. Thus we learn that $p_1^2 | m^2 = n^2 p_1, \dots, p_k$ and therefore that $p_1 | n^2$. Another application of Euclid's lemma shows $p_1 | n$. Thus we have shown that p_1 is a divisor of both m and n contradicting the fact that m and n were relatively prime. Thus we must conclude that $b = 0 = a$. Therefore $a^2 - b^2\delta = 0$ only if $a = 0 = b$. ■

Later on we will show the following;

Fact 6.3 *Suppose that $\theta \in \mathbb{C}$ is the root of some polynomial in $\mathbb{Q}[x]$, then $\mathbb{Q}[\theta]$ is a sub-field of $\mathbb{C}$.*

Recall that we already know $\mathbb{Q}[\theta]$ is an integral domain. To prove that $\mathbb{Q}[\theta]$ is a field we will have to show that for every nonzero $z \in \mathbb{Q}[\theta]$ that the inverse, $z^{-1} \in \mathbb{C}$, is actually back in $\mathbb{Q}[\theta]$.

6.2 Homomorphisms

Definition 6.4. *Let R and S be rings. A function $\varphi : R \to S$ is a* ***homomorphism*** *if*

$$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) \text{ and}$$
$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$$

for all $r_1, r_2 \in R$. That is, φ preserves addition and multiplication. If we further assume that φ is an invertible map (i.e. one to one and onto), then we say $\varphi : R \to S$ is an ***isomorphism*** *and that R and S are* ***isomorphic.***

Example 6.5 (Conjugation isomorphism). Let $\varphi : \mathbb{C} \to \mathbb{C}$ be defined by $\varphi(z) = \bar{z}$ where for $z = x + iy$, $\bar{z} := x - iy$ is the complex conjugate of z. Then it is routine to check that φ is a ring isomorphism. Notice that $z = \bar{z}$ iff $z \in \mathbb{R}$. There is analogous conjugation isomorphism on $\mathbb{Q}[i]$, $\mathbb{Z}[i]$, and $\mathbb{Z}_m[i]$ (for $m \in \mathbb{Z}_+$) with similar properties.

Here is another example in the same spirit of the last example.

Example 6.6 (Another conjugation isomorphism). Let $\varphi : \mathbb{Q}\left[\sqrt{2}\right] \to \mathbb{Q}\left[\sqrt{2}\right]$ be defined by

$$\varphi\left(a + b\sqrt{2}\right) = a - b\sqrt{2} \text{ for all } a, b \in \mathbb{Q}.$$

Then φ is a ring isomorphism. Again this is routine to check. For example,

$$\begin{aligned}\varphi\left(a + b\sqrt{2}\right)\varphi\left(u + v\sqrt{2}\right) &= \left(a - b\sqrt{2}\right)\left(u - v\sqrt{2}\right) \\ &= au + 2bv - (av + bu)\sqrt{2}\end{aligned}$$

while

$$\begin{aligned}\varphi\left(\left(a + b\sqrt{2}\right)\left(u + v\sqrt{2}\right)\right) &= \varphi\left(au + 2bv + (av + bu)\sqrt{2}\right) \\ &= au + 2bv - (av + bu)\sqrt{2}.\end{aligned}$$

Notice that for $\xi \in \mathbb{Q}\left[\sqrt{2}\right]$, $\varphi(\xi) = \xi$ iff $\xi \in \mathbb{Q}$.

Example 6.7. The only ring homomorphisms, $\varphi : \mathbb{Z} \to \mathbb{Z}$ are $\varphi(a) = a$ and $\varphi(a) = 0$ for all $a \in \mathbb{Z}$. Indeed, if $\varphi : \mathbb{Z} \to \mathbb{Z}$ is a ring homomorphism and $t := \varphi(1)$, then $t^2 = \varphi(1)\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) = t$. The only solutions to $t^2 = t$ in $\mathbb{Z}$ are $t = 0$ and $t = 1$. In the first case $\varphi \equiv 0$ and in the second $\varphi = id$.

Lecture 7

Example 7.1. Suppose that $g \in M_2(\mathbb{R})$ is a unit, i.e. g^{-1} exists. Then $\varphi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ defined by,

$$\varphi(A) := gAg^{-1} \text{ for all } A \in M_2(\mathbb{R}),$$

is a ring isomorphism. For example,

$$\varphi(A)\varphi(B) = \left(gAg^{-1}\right)\left(gBg^{-1}\right) = gAg^{-1}gBg^{-1} = gABg^{-1} = \varphi(AB).$$

Observe that $\varphi^{-1}(A) = g^{-1}Ag$ and $\varphi(I) = I$.

Proposition 7.2 (Homomorphisms from $\mathbb{Z}$). *Suppose that R is a ring and $a \in R$ is an element such that $a^2 = a$. Then there exists a unique ring homomorphism, $\varphi : \mathbb{Z} \to R$ such that $\varphi(1) = a$. Moreover, $\varphi(k) = k \cdot a$ for all $k \in \mathbb{Z}$.*

Proof. Recall from last quarter that, $\varphi(n) := n \cdot a$ for all $n \in \mathbb{Z}$ is a group homomorphism. This is also a ring homomorphism since,

$$\varphi(m)\varphi(n) = (m \cdot a)(n \cdot a) = mn \cdot a^2 = mn \cdot a = \varphi(mn),$$

wherein we have used Corollary 5.6 for the second equality. ■

Corollary 7.3. *Suppose that R is a ring with $1_R \in R$. Then there is a unique homomorphism, $\varphi : \mathbb{Z} \to R$ such that $\varphi(1_{\mathbb{Z}}) = 1_R$.*

Proposition 7.4. *Suppose that $\varphi : R \to S$ is a ring homomorphism. Then;*

1. $\varphi(0) = 0$,
2. $\varphi(-r) = -\varphi(r)$ *for all* $r \in R$,
3. $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$ *for all* $r_1, r_2 \in R$.
4. *If $1_R \in R$ and φ is surjective, then $\varphi(1_R)$ is an identity in S.*
5. *If $\varphi : R \to S$ is an isomorphism of rings, then $\varphi^{-1} : S \to R$ is also a isomorphism.*

Proof. Noting that $\varphi : (R, +) \to (S, +)$ is a group homomorphism, it follows that items 1. – 3. were covered last quarter when we studied groups. The proof of item 5. is similar to the analogous statements for groups and hence will be omitted. So let me prove item 4. here.

To each $s \in S$, there exists $a \in R$ such that $\varphi(a) = s$. Therefore,

$$\begin{gathered}\varphi(1_R)s = \varphi(1_R)\varphi(a) = \varphi(1_R a) = \varphi(a) = s \\ \text{and} \\ s\varphi(1_R) = \varphi(a)\varphi(1_R) = \varphi(a1_R) = \varphi(a) = s.\end{gathered}$$

Since these equations hold for all $s \in S$, it follows that $\varphi(1_R)$ is an (the) identity in S. ■

Definition 7.5. *As usual, if $\varphi : R \to S$ is a ring homomorphism we let*

$$\ker(\varphi) := \{r \in R : \varphi(r) = 0\} = \varphi^{-1}(\{0_S\}) \subset R.$$

Lemma 7.6. *If $\varphi : R \to S$ is a ring homomorphism, then* $\ker(\varphi)$ *is an ideal of R.*

Proof. We know from last quarter that $\ker(\varphi)$ is a subgroup of $(R, +)$. If $r \in R$ and $n \in \ker(\varphi)$, then

$$\begin{aligned}\varphi(rn) &= \varphi(r)\varphi(n) = \varphi(r)0 = 0 \text{ and} \\ \varphi(nr) &= \varphi(n)\varphi(r) = 0\varphi(r) = 0,\end{aligned}$$

which shows that rn and $nr \in \ker(\varphi)$ for all $r \in R$ and $n \in \ker(\varphi)$. ■

Example 7.7. Let us find all of the ring homomorphisms, $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ and their kernels. To do this let $t := \varphi(1)$. Then $t^2 = \varphi(1)\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) = t$. The only solutions to $t^2 = t$ in $\mathbb{Z}_{10}$ are $t = 0$, $t = 1$, $t = 5$ and $t = 6$.

1. If $t = 0$, then $\varphi \equiv 0$ and $\ker(\varphi) = \mathbb{Z}$.
2. If $t = 1$, then $\varphi(x) = x \bmod 10$ and $\ker\varphi = \langle 10 \rangle = \langle 0 \rangle = \{0\} \subset \mathbb{Z}$.
3. If $t = 5$, then $\varphi(x) = 5x \bmod 10$ and $x \in \ker\varphi$ iff $10|5x$ iff $2|x$ so that $\ker(\varphi) = \langle 2 \rangle = \{0, 2, 4, 8\}$.
4. If $t = 6$, then $\varphi(x) = 6x \bmod 10$ and $x \in \ker\varphi$ iff $10|6x$ iff $5|x$ so that $\ker(\varphi) = \langle 5 \rangle = \{0, 5\} \subset \mathbb{Z}$.

Proposition 7.8. *Suppose $n \in \mathbb{Z}_+$, R is a ring, and $a \in R$ is an element such that $a^2 = a$ and $n \cdot a = 0$. Then there is a unique homomorphism, $\varphi : \mathbb{Z}_n \to R$ such that $\varphi(1) = a$ and in fact $\varphi(k) = k \cdot a$ for all $k \in \mathbb{Z}_n$.*

Proof. This has a similar proof to the proof of Proposition 7.2. ■

Corollary 7.9. *Suppose that R is a ring, $1_R \in R$, and $\operatorname{chr}(R) = n \in \mathbb{Z}_+$. Then there is a unique homomorphism, $\varphi : \mathbb{Z}_n \to R$ such that $\varphi(1_{\mathbb{Z}_n}) = 1_R$ which is given by $\varphi(m) = m \cdot 1_R$ for all $m \in \mathbb{Z}_n$. Moreover, $\ker(\varphi) = \langle 0 \rangle = \{0\}$.*

Example 7.10. Suppose that $\varphi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ is a ring homomorphism and $t := \varphi(1)$. Then $t^2 = \varphi(1)^2 = \varphi(1) = t$, and therefore $t^2 = t$. Moreover we must have $0 = \varphi(0) = \varphi(10 \cdot 1) = 10 \cdot t$ which is not restriction on t. As we have seen the only solutions to $t^2 = t$ in $\mathbb{Z}_{10}$ are $t = 0$, $t = 1$, $t = 5$ and $t = 6$. Thus φ must be one of the following; $\varphi \equiv 0$, $\varphi = id$, $\varphi(x) = 5x$, or $\varphi(x) = 6x$ for all $x \in \mathbb{Z}_{10}$. The only ring isomorphism is the identity in this case. If $\varphi(x) = 5x$

Example 7.11. Suppose that $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{10}$ is a ring homomorphism and let $t := \varphi(1)$. Then as before, $t^2 = t$ and this forces $t = 0, 1, 5,$ or 6. In this case we must also require $12 \cdot t = 0$, i.e. $10|12 \cdot t$, i.e. $5|t$. Therefore we may now only take $t = 0$ or $t = 5$, i.e.

$$\varphi(x) = 0 \text{ for all } x \in \mathbb{Z}_{12} \text{ or}$$
$$\varphi(x) = 5x \bmod 10 \text{ for all } x \in \mathbb{Z}_{12}$$

are the only such homomorphisms.

Theorem 7.12 (Not covered in class). *If $\varphi : \mathbb{R} \to \mathbb{R}$ is a ring homomorphism, then φ is either the zero or the identity homomorphism.*

Proof. If $t = \varphi(1)$, then as above, $t^2 = t$, i.e. $t(t-1) = 0$. Since $\mathbb{R}$ is a field this implies that $t = 0$ or $t = 1$. If $t = 0$, then for all $a \in \mathbb{R}$,

$$\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = \varphi(a) \cdot 0 = 0,$$

i.e. φ is the zero homomorphism. So we may now assume that $t = 1$.

If $t = 1$,

$$\varphi(n) = \varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot 1 = n$$

for all $n \in \mathbb{Z}$. Therefore for $n \in \mathbb{N} \setminus \{0\}$ and $m \in \mathbb{Z}$,

$$m = \varphi(m) = \varphi\left(n \cdot \frac{m}{n}\right) = \varphi(n)\varphi\left(\frac{m}{n}\right) = n\varphi\left(\frac{m}{n}\right)$$

from which it follows that $\varphi(m/n) = m/n$. Thus we now know that $\varphi|_{\mathbb{Q}}$ is the identity.

Since $\ker(\varphi) \neq \mathbb{R}$, we must have $\ker(\varphi) = \{0\}$ so that φ is injective. In particular $\varphi(b) \neq 0$ for all $b \neq 0$. Moreover if $a > 0$ in $\mathbb{R}$ and $b := \sqrt{a}$, then

$$\varphi(a) = \varphi(b^2) = [\varphi(b)]^2 > 0.$$

So if $y, x \in \mathbb{R}$ with $y > x$, then $\varphi(y) - \varphi(x) = \varphi(y - x) > 0$, i.e. φ is order preserving.

Finally, let $a \in \mathbb{R}$ and choose rational numbers $x_n, y_n \in \mathbb{Q}$ such that $x_n < a < y_n$ with $x_n \uparrow a$ and $y_n \downarrow a$ as $n \to \infty$. Then

$$x_n = \varphi(x_n) < \varphi(a) < \varphi(y_n) = y_n \text{ for all } n.$$

Letting $n \to \infty$ in this last equation then shows, $a \leq \varphi(a) \leq a$, i.e. $\varphi(a) = a$. Since $a \in \mathbb{R}$ was arbitrary, we may conclude that φ is the identity map on $\mathbb{R}$. ■

Lecture 8

Remark 8.1 (Comments on ideals). Let me make two comments on ideals in a commutative ring, R.

1. To check that a non-empty subset, $S \subset R$, is an ideal, we should show $(S,+)$ is a subgroup of R and that $RS \subset S$. Since R is commutative, you do not have to also show $SR \subset S$. This is because $RS = SR$ in when R is commutative.
2. If $a \in R$, the **principle ideal generated by** a is defined by;

$$\langle a \rangle := Ra = \{ra : r \in R\}.$$

It is easy to check that this is indeed an ideal. So for example if $R = \mathbb{R}[x]$ then $\langle x \rangle = \mathbb{R}[x] \cdot x$ which is the same as the polynomials without a constant term, i.e. $p(x) = a_1 x + a_2 x^2 + \dots + a_n x^n$. The coefficient $a_0 = 0$. Similarly, $\left\langle x^2+1 \right\rangle = \mathbb{R}[x]\left(x^2+1\right)$ is the collection of all polynomials which contain $\left(x^2+1\right)$ as a factor.

Recall from last time:

1. If $a \in R$ satisfies $a^2 = a$, then $\varphi(k) := k \cdot a$ is a ring homomorphism from $\mathbb{Z} \to R$.
2. If we further assume that $n \cdot a = 0$ for some $n \in \mathbb{Z}_+$, then $\varphi(k) := k \cdot a$ also defines a ring homomorphism from $\mathbb{Z}_n \to R$.

Example 8.2. For any $m > 1$, $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ given by $\varphi(a) = a \cdot 1_{\mathbb{Z}_m} = a \bmod m$ is a ring homomorphism. This also follows directly from the properties of the $(\cdot) \bmod m$ – function. In this case $\ker(\varphi) = \langle m \rangle = \mathbb{Z}m$.

Example 8.3. If $n \in \mathbb{Z}_+$ and $m = kn$ with $k \in \mathbb{Z}_+$, then there is a unique ring homomorphisms, $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$ such that $\varphi(1_m) = 1_n$. To be more explicit,

$$\varphi(a) = \varphi(a \cdot 1_m) = a \cdot \varphi(1_m) = a \cdot 1_n = (a \bmod n) \cdot 1_n = a \bmod n.$$

Example 8.4. In $\mathbb{Z}_{10}$, the equation, $a^2 = a$ has a solutions $a = 5$ and $a = 6$. Notice that $|5| = 2$ and $|6| = |\gcd(10,6)| = |2| = 5$. Thus we know that for any $k \geq 1$ there are ring homomorphisms, $\varphi : \mathbb{Z}_{5k} \to \mathbb{Z}_{10}$ and $\psi : \mathbb{Z}_{2k} \to \mathbb{Z}_{10}$ such that

$$\varphi(1_{5k}) = 6 \text{ and } \psi(1_{2k}) = 5.$$

As before, one shows that

$$\varphi(m) = m \cdot 6 = (6m) \bmod 10 \text{ and } \psi(m) = m \cdot 5 = (5m) \bmod 10.$$

Example 8.5 (Divisibility tests). Let $n = a_k a_{k-1} \dots a_0$ be written in decimal form, so that

$$n = \sum_{i=0}^{k} a_i 10^i. \tag{8.1}$$

Applying the ring homomorphism, mod 3 and mod 9 to this equation shows,

$$\begin{aligned} n \bmod 3 &= \sum_{i=0}^{k} a_i \bmod 3 \cdot (10 \bmod 3)^i \\ &= \left(\sum_{i=0}^{k} a_i\right) \bmod 3 \end{aligned}$$

and similarly,

$$n \bmod 9 = \sum_{i=0}^{k} a_i \bmod 9 \cdot (10 \bmod 9)^i = \left(\sum_{i=0}^{k} a_i\right) \bmod 9.$$

Thus we learn that $n \bmod 3 = 0$ iff $\left(\sum_{i=0}^{k} a_i\right) \bmod 3 = 0$ i.e. $3|n$ iff $3|\left(\sum_{i=0}^{k} a_i\right)$. Similarly, since $10 \bmod 9 = 1$, the same methods show $9|n$ iff $9|\left(\sum_{i=0}^{k} a_i\right)$. (See the homework problems for more divisibility tests along these lines. Also consider what this test gives if you apply mod 2 to Eq. (8.1).)

Theorem 8.6. *Let R be a commutative ring with $1 \in R$. To each $a \in R$ with $a^2 + 1 = 0$, there is a unique ring homomorphism $\varphi : \mathbb{Z}[i] \to R$ such that $\varphi(1) = 1$ and $\varphi(i) = a$.*

Proof. Since $\mathbb{Z}[i]$ is generated by i, we see that φ is completely determined by $a := \varphi(i) \in R$. Now we can not choose a arbitrarily since we must have

$$a^2 = \varphi(i)^2 = \varphi\left(i^2\right) = \varphi(-1) = -1_R,$$

i.e. $a^2 + 1 = 0$.

Conversely given $a \in R$ such that $a^2 + 1 = 0$, we should define

$$\varphi(x + iy) = x1 + ya \text{ for all } x, y \in \mathbb{Z},$$

where $ya = a + a + \cdots + a - y$ times. The main point in checking that φ is a homomorphism is to show it preserves the multiplication operation of the rings. To check this, let $x, y, u, v \in \mathbb{Z}$ and consider;

$$\varphi((x + iy)(u + iv)) = \varphi(xu - yv + i(xv + yu)) = (xu - yv) 1_R + (xv + yu) a.$$

On the other hand

$$\begin{aligned}
\varphi(x + iy) \varphi(u + iv) &= (x1_R + ya)(u1_R + va) \\
&= (x1_R + ya)(u1_R + va) \\
&= xu1_R + yva^2 + yua + xva \\
&= (xu - yv) 1_R + (yu + xv) a \\
&= \varphi((x + iy)(u + iv)).
\end{aligned}$$

Thus we have shown $\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta)$ for all $\xi, \eta \in \mathbb{Z}[i]$. The fact that $\varphi(\xi + \eta) = \varphi(\xi) + \varphi(\eta)$ is easy to check and is left to the reader. ■

Remark 8.7. This could be generalized by supposing that $a, b \in R$ with $b^2 = b$ and $a^2 + b = 0$. Then we would have $\varphi(x + yi) = x \cdot b + y \cdot a$ would be the desired homomorphism. Indeed, let us observe that

$$\begin{aligned}
\varphi(x + iy) \varphi(u + iv) &= (xb + ya)(ub + va) \\
&= (xb + ya)(ub + va) \\
&= xub^2 + yva^2 + yua + xva \\
&= (xu - yv) b + (yu + xv) a \\
&= \varphi((x + iy)(u + iv)).
\end{aligned}$$

Example 8.8. Let $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_3[i]$ be the unique homomorphism such that $\varphi(1) = 1$ and $\varphi(i) = i$, i.e.

$$\varphi(a + ib) = a \cdot 1 + b \cdot i = a \bmod 3 + (b \bmod 3) i \in \mathbb{Z}_3[i].$$

Notice that

$$\ker(\varphi) = \{a + bi : a, b \in \langle 3 \rangle \subset \mathbb{Z}\} = \langle 3 \rangle + \langle 3 \rangle i.$$

Here is a more interesting example.

Example 8.9. In $\mathbb{Z}_{10}$ we observe that $3^2 = 9 = -1$ and also $7 = -3$ has this property, namely $7^2 = (-3)^2 = 3^2 = 9 = -1$. Therefore there exists a unique homomorphism, $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{10}$ such that $\varphi(1) = 1$ and $\varphi(i) = 7 = -3$. The explicit formula is easy to deduce,

$$\varphi(a + bi) = a \cdot 1 + b \cdot 7 = (a - 3b) \bmod 10.$$

Lecture 9

Lemma 9.1. *If $\varphi : R \to S$ is a ring homomorphism, then* $\ker(\varphi)$ *is an ideal of* R.

Proof. We know from last quarter that $\ker(\varphi)$ is a subgroup of $(R,+)$. If $r \in R$ and $n \in \ker(\varphi)$, then

$$\varphi(rn) = \varphi(r)\varphi(n) = \varphi(r)0 = 0 \text{ and}$$
$$\varphi(nr) = \varphi(n)\varphi(r) = 0\varphi(r) = 0,$$

which shows that rn and $nr \in \ker(\varphi)$ for all $r \in R$ and $n \in \ker(\varphi)$. ∎

Example 9.2. If $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ is the ring homomorphism defined by $\varphi(a) := a \bmod m$, then

$$\ker\varphi = \{a \in \mathbb{Z} : a \bmod m = 0\} = \mathbb{Z}m = \langle m \rangle.$$

We will see many more examples of Lemma 9.1 below.

9.1 Factor Rings

Definition 9.3. *Let R be a ring, $I \subset R$ an ideal. The factor ring R/I is defined to be*

$$R/I := \{r + I : r \in R\}$$

with operations

$$(a+I) + (b+I) := (a+b) + I \text{ and}$$
$$(a+I)(b+I) := (ab) + I.$$

We may also write $[a]$ for $a + I$ in which cases the above equations become,

$$[a] + [b] := [a+b] \text{ and } [a][b] := [ab].$$

Theorem 9.4. *A factor ring really is a ring.*

Proof. The elements of R/I are the left cosets of I in the group $(R,+)$. There is nothing new here. R/I is itself a group with the operation $+$ defined by $(a+I) + (b+I) = (a+b) + I$. This follows from last quarter as $I \subset R$ is a normal subgroup of $(R,+)$ since $(R,+)$ is abelian. So we only need really to check that the definition of product makes sense.

Problem: we are multiplying coset representatives. We have to check that the resulting coset is independent of the choice of representatives. Thus we need to show; if $a, b, a', b' \in R$ with

$$a + I = a' + I \text{ and } b + I = b' + I,$$

then $ab + I = a'b' + I$. By definition of cosets, we have $i := a - a' \in I$ and $j := b - b' \in I$. Therefore,

$$ab = (a' + i)(b' + j) = a'b' + ib' + a'j + ij \in a'b' + I$$

since $ib' + a'j + ij \in I$ because I is an ideal. So indeed, $ab + I = a'b' + I$ and we have a well defined product on R/I. Checking that product is associative and the distributive laws is easy and will be omitted. ∎

Example 9.5. Suppose that $I = \langle 4 \rangle = \mathbb{Z} \cdot 4 \subset \mathbb{Z}$. In this case, if $a \in \mathbb{Z}$ then $a - a \bmod 4 \in I$ and therefore,

$$[a] = a + I = a \bmod 4 + I = [a \bmod 4].$$

Moreover if $0 \le a, b \le 3$ with $a + I = b + I$ then $a - b \in I$, i.e. $a - b$ is a multiple of 4. Since $|a - b| < 4$, this is only possible if $a = b$. Thus if we let $\mathcal{S} = \{0,1,2,3\}$, then

$$\mathbb{Z}/\langle 4 \rangle = \{[m] = m + \langle 4 \rangle : m \in \mathcal{S}\} = [\mathcal{S}].$$

Moreover, we have

$$[a][b] = [ab] = [(ab) \bmod 4]$$

and

$$[a] + [b] = [a+b] = [(a+b) \bmod 4].$$

Thus the induced ring structure on $\mathcal{S}$ is precisely that of $\mathbb{Z}_4$ and so we may conclude;

$$\mathbb{Z}_4 \ni a \to [a] = a + \langle 4 \rangle \in \mathbb{Z}/\langle 4 \rangle$$

is a ring isomorphism.

Lecture 10

Remark 10.1. Roughly speaking, you should think of R/I being R with the proviso that we identify two elements of R to be the same if they differ by an element from I. To understand R/I in more concrete terms, it is often useful to look for subset, $\mathcal{S} \subset R$, such that the map,

$$\mathcal{S} \ni a \to a + I \in R/I$$

is a bijection. (We will call such an $\mathcal{S}$ a slice.) This allows us to identify R/I with $\mathcal{S}$ and this identification induces a ring structure on $\mathcal{S}$. We will see how this goes in the examples below. **Warning:** the choice of a slice $\mathcal{S}$ is highly non-unique although there is often a "natural" choice in a given example. The point is to make $\mathcal{S}$ we need only choose one element from each of the cosets in R/I.

Example 9.5 easily generalizes to give the following theorem. We will give another proof shortly using the first isomorphism theorem, see 10.4 below.

Theorem 10.2 ($\mathbb{Z}_m \cong \mathbb{Z}/\langle m\rangle$). *For all $m \geq 2$, the map,*

$$\mathbb{Z}_m \ni a \to [a] = a + \langle m\rangle \in \mathbb{Z}/\langle m\rangle \tag{10.1}$$

is a ring isomorphism.

Proof. The distinct cosets of $\mathbb{Z}/\langle m\rangle$ are given by

$$\{[k] = k + \langle m\rangle : k = 0, 1, 2 \ldots, m-1\}$$

and therefore we may take $\mathcal{S} = \mathbb{Z}_m$. Since $[a] = [a \bmod m]$, it is easy to see that the map in Eq. (10.1) is a ring isomorphism. ∎

10.1 First Isomorphism Theorem

Recall that two rings, R and S (written $R \cong S$) are isomorphic, if there is a ring isomorphism, $\varphi : R \to S$. That is φ should be a one-to-one and onto ring homomorphism.

Theorem 10.3 (First Isomorphism Theorem). *Let R and S be rings and $\varphi : R \to S$ be a homomorphism. Let*

$$\varphi(R) = \operatorname{Ran}\varphi = \{\varphi(r) : r \in R\} \subset S$$

and recall that $I = \ker\varphi := \{r \in R : \varphi(r) = 0\}$ is an ideal in R. Then $\varphi(R)$ is a subring of S and $\bar{\varphi} : R/I \to \varphi(R)$ defined by

$$\bar{\varphi}([r]) = \bar{\varphi}(r + I) := \varphi(r) \text{ for all } r \in R$$

is a ring isomorphism.

Proof. We have seen last quarter that $\bar{\varphi} : R/\ker\varphi \to \varphi(R)$ is an (additive) group isomorphism. So it only remains to show $\bar{\varphi}$ preserves the multiplication operations on $\varphi(R)$ and R/I which goes as follows;

$$\begin{aligned}\bar{\varphi}([a])\,\bar{\varphi}([b]) &= \varphi(a)\,\varphi(b) \\ &= \varphi(ab) = \bar{\varphi}([ab]) = \bar{\varphi}([a]\,[b]).\end{aligned}$$

∎

Example 10.4 ($\mathbb{Z}/(\mathbb{Z}m) \cong \mathbb{Z}_m$). Let $m \in \mathbb{Z}_+$ and $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ be the ring homomorphism, $\varphi(x) = x \bmod m$. Since $\varphi(\mathbb{Z}) = \mathbb{Z}_m$ and $\ker(\varphi) = \langle m\rangle = \mathbb{Z}m$, the first isomorphism theorem implies, $\bar{\varphi} : \mathbb{Z}/(\mathbb{Z}m) \to \mathbb{Z}_m$ is a ring isomorphism where $\bar{\varphi}([a]) = \varphi(a) = a \bmod m$ for all $a \in \mathbb{Z}$.

Example 10.5. Let us consider $R := \mathbb{Z}[i]/\langle i-2\rangle$. In this ring $[i-2] = 0$ or equivalently, $[i] = [2]$. Squaring this equation also shows,

$$[-1] = \left[i^2\right] = [i]^2 = [2]^2 = \left[2^2\right] = [4]$$

from which we conclude that $[5] = 0$, i.e. $5 \in \langle i-2\rangle$. This can also be seen directly since $5 = -(i+2)(i-2) \in \langle i-2\rangle$. Using these observations we learn for $a + ib \in \mathbb{Z}[i]$ that

$$[a + ib] = [a + 2b] = [(a + 2b) \bmod 5].$$

Thus, if we define $\mathcal{S} = \{0, 1, 2, 3, 4\}$, we have already shown that

$$R = \{[a] : a \in \mathcal{S}\} = [\mathcal{S}] \,.$$

Now suppose that $a, b \in \mathcal{S}$ with $[a] = [b]$, i.e. $0 = [a-b] = [c]$ where $c = (a-b) \bmod 5$. Since $c \in \langle i-2 \rangle$ we must have

$$c = (i-2)(a+bi) = -(2a+b) + (a-2b)\, i$$

from which it follows that $a = 2b$ and

$$c = -(2a+b) = -5b.$$

Since $0 \leq c < 5$, this is only possible if $c = 0$ and therefore,

$$a = a \bmod 5 = b \bmod 5 = b.$$

Finally let us now observe that

$$\begin{aligned} [a] + [b] &= [a+b] = [(a+b) \bmod 5] \text{ and} \\ [a] \cdot [b] &= [ab] = [(ab) \bmod 5] \end{aligned}$$

so that the induced ring structure on $\mathcal{S}$ is the same a the ring structure on $\mathbb{Z}_5$. Hence we have proved,

$$\mathbb{Z}_5 \ni a \to [a] = a + \langle i-2 \rangle \in \mathbb{Z}[i] \,/\, \langle i-2 \rangle$$

is an isomorphism of rings.

Lecture 11

Example 11.1 (Example 10.5 revisited). In $\mathbb{Z}_5$, we see that $2^2 = 4 = -1$ and therefore there is a ring homomorphism, $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5$ such that $\varphi(1) = 1$ and $\varphi(i) = 2$. More explicitly we have,

$$\varphi(a + bi) = a \cdot 1 + b \cdot 2 = (a + 2b) \bmod 5.$$

Moreover, $(a + ib) \in \ker(\varphi)$ iff $a + 2b = 5k$ for some $k \in \mathbb{Z}$ and therefore,

$$\ker(\varphi) = \{-2b + 5k + ib : b, k \in \mathbb{Z}\} = \mathbb{Z}(2 - i) + \mathbb{Z} \cdot 5.$$

Since $(2 + i)(2 - i) = 5$ and $2 - i \in \ker(\varphi)$, we have, and

$$\langle 2 - i \rangle \subset \ker(\varphi) = \mathbb{Z}(2 - i) + \mathbb{Z} \cdot 5 \subset \langle 2 - i \rangle$$

from which it follows that $\ker(\varphi) = \langle 2 - i \rangle$. Thus by the first isomorphism theorem, $\bar{\varphi} : \mathbb{Z}[i] / \langle 2 - i \rangle \to \mathbb{Z}_5$ defined by

$$\bar{\varphi}([a + ib]) = \varphi(a + bi) = (a + 2b) \bmod 5$$

is a ring isomorphism. Notice that the inverse isomorphism is given by $\bar{\varphi}^{-1}(a) = [a]$ for all $a \in \mathbb{Z}_5$ which should be compared with Example 10.5 above.

For what follows recall that the evaluation maps are homomorphisms.

Theorem 11.2 (Evaluation homomorphism). *Let R be a subring of a commutative ring, $\bar{R}$, and $t \in \bar{R}$. Then there exists a ring homomorphism, $\varphi_t : R[x] \to \bar{R}$ such that*

$$\varphi_t(p) = \sum_{k=0}^{n} a_k t^k \text{ when } p(x) = \sum_{k=0}^{n} a_k x^k \in R[x].$$

We will usually simply write $p(t)$ for $\varphi_t(p)$.

The hole point of how we define polynomial multiplication is to make this theorem true. We will give the formal proof of this theorem a bit later in the notes.

Example 11.3. Let $I := \langle x \rangle = \mathbb{R}[x]\, x \subset \mathbb{R}[x]$ from which it follows that $[x] = 0 \in \mathbb{R}[x] / \langle x \rangle$. Therefore if $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, then

$$[p(x)] = [a_0 + a_1 x + \cdots + a_n x^n] = [a_0].$$

Alternatively put, $p(x) + I = a_0 + I$ since $a_1 x + \cdots + a_n x^n \in I$. Moreover, if $[a_0] = [b_0]$, then $a_0 - b_0 \in I$ which can happen iff $a_0 = b_0$. Therefore we may identify $\mathbb{R}[x] / \langle x \rangle$ with $\mathcal{S} = \mathbb{R}$ thought of as the constant polynomials inside of $\mathbb{R}[x]$. In fact it is easy to check that

$$\mathbb{R} \ni a \to a + I \in \mathbb{R}[x] / \langle x \rangle$$

is a ring isomorphism.

Alternatively we may use the first isomorphism theorem as follows. Let $\varphi(p) := p(0)$, then $\varphi : \mathbb{R}[x] \to \mathbb{R}$ is a ring homomorphism onto $\mathbb{R}$ with $\ker(\varphi) = \langle x \rangle$. Therefore, $\bar{\varphi} : \mathbb{R}[x] / \langle x \rangle \to \mathbb{R}$ is a ring isomorphism.

Theorem 11.4 (Division Algorithm). *Let $F[x]$ be a polynomial ring where F is a field. Given $f, g \in F[x]$ both nonzero, there exists a unique $q, r \in F[x]$ with $f = qg + r$ such that either $r = 0$ or $\deg r < \deg g$.*

Interpretation. We are dividing f by g and so g **goes into** f, q **times with remainder** r. This is really high school polynomial division which we will discuss in more detail a bit later. In the sequel we will sometimes denote the remainder, r by $f \bmod g$.

Corollary 11.5. *Suppose that F is a field, $p(x) = c_0 + \cdots + c_n x^n \in F[x]$ is a polynomial with $c_n \neq 0$, and let*

$$\mathcal{S} := \left\{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} : a_i \in F \text{ for } i = 0, 1, \ldots, n-1\right\}.$$

Then the map, $\varphi : \mathcal{S} \to F[x] / \langle p \rangle$ defined by

$$\varphi(f) = [f] := f + \langle p \rangle \text{ for all } f \in \mathcal{S}$$

is a bijection. Moreover, $\mathcal{S}$ becomes a ring and φ a ring homomorphism provided we define

$$f(x) \cdot g(x) := [f(x)\, g(x)] \bmod p$$

and $f + g$ as usual polynomial addition.

Proof. 1. If $f \in F[x]$, then by the division algorithm

$$f = qp + r = qp + f \bmod p$$

and therefore,

$$[f] = [qp + r] = [q][p] + [r] = [q]\,0 + [r] = [r].$$

Thus we have shown

$$[f] = [f \bmod p] \text{ for all } f \in F[x]. \tag{11.1}$$

2. Equation (11.1) shows $\varphi : \mathcal{S} \to F[x] / \langle p \rangle$ is onto. To see φ is injective, suppose that $f, g \in \mathcal{S}$ and $\varphi(f) = \varphi(g)$. Then $[f-g] = 0$, i.e. $f - g \in \langle p \rangle$, i.e. $f - g = q \cdot p$ for some $q \in F[x]$. However this is impossible unless $q = 0$ and $f = g$ since otherwise,

$$n - 1 \geq \deg(f-g) = \deg(q) + \deg(p) = \deg(q) + n.$$

Thus we have shown φ is injective as well, i.e. $\varphi : \mathcal{S} \to F[x] / \langle p \rangle$ is a bijection.

3. Making use of Eq. (11.1) and the fact that φ is a bijection shows,

$$\varphi(f)\varphi(g) = [f][g] = [fg] = [(fg) \bmod p] = \varphi((fg) \bmod p) \text{ and}$$
$$\varphi(f) + \varphi(g) = [f] + [g] = [f+g] = \varphi(f+g)$$

for all $f, g \in \mathcal{S}$. Thus $\mathcal{S}$ equipped with the operations described in the theorem makes $\mathcal{S}$ into a ring for which φ is a ring isomorphism. ∎

Theorem 11.6 ($\mathbb{C}$ as a factor ring). $\mathbb{C} \cong \mathbb{R}[x] / \langle x^2 + 1 \rangle =: R$. *The maps,*

$$\mathbb{C} \ni (a + ib) \to [a + bx] \in \mathbb{R}[x] / \langle x^2 + 1 \rangle \text{ and}$$
$$\mathbb{R}[x] / \langle x^2 + 1 \rangle \ni [p(x)] = p(x) + \langle x^2 + 1 \rangle \to p(i) \in \mathbb{C}$$

are ring isomorphisms which are inverses to one another.

Proof. We are going to give two proofs that $\mathbb{C} \cong \mathbb{R}[x] / \langle x^2 + 1 \rangle$. Our first proof gives rise to the first map while our second gives rise to the second map.

First Proof. Let $\mathcal{S} = \{a + bx : x, b \in \mathbb{R}\}$ so that

$$\mathcal{S} \ni (a + bx) \to [a + bx] \in \mathbb{R}[x] / \langle x^2 + 1 \rangle$$

is a bijection. Since $[x^2 + 1] = 0$, we have $[x^2] = [-1]$ and therefore,

$$\begin{aligned}[a + bx][c + dx] &= [ac + (bc + ad)x + bdx^2] \\ &= [ac + (bc + ad)x + bd(-1)] \\ &= [ac - bd + (bc + ad)x].\end{aligned}$$

Moreover one easily shows,

$$[a + bx] + [c + dx] = [(a + c) + (b + d)x].$$

From these two facts it is now easy to check that

$$\mathbb{C} \ni (a + ib) \to [a + bx] \in R$$

is an isomorphism of rings.

Second Proof. Let $\varphi : \mathbb{R}[x] \to \mathbb{C}$ be the evaluation homomorphism, $\varphi(p) = p(i)$ where $i = \sqrt{-1} \in \mathbb{C}$. We then have $\varphi(\mathbb{R}[x]) = \mathbb{R}[i] = \mathbb{C}$ and so by the first isomorphism theorem, $\mathbb{R}[x] / \ker(\varphi) \cong \mathbb{C}$. So to finish the proof we must show,

$$\ker(\varphi) = \langle x^2 + 1 \rangle = \mathbb{R}[x](x^2 + 1). \tag{11.2}$$

Suppose that $p \in \ker(\varphi)$ and use the division algorithm to write,

$$p(x) = q(x)(x^2 + 1) + r(x) \text{ where}$$
$$r(x) = a + bx \text{ for some } a, b \in \mathbb{R}.$$

As $p(i) = 0$ and $i^2 + 1 = 0$, it follows that $r(i) = a + bi = 0$. But this happens iff $a = 0 = b$, and therefore we see that $r \equiv 0$ an hence that $p(x) \in \langle x^2 + 1 \rangle$. Thus we have shown $\ker(\varphi) \subset \langle x^2 + 1 \rangle$ and since $x^2 + 1 \in \ker(\varphi)$ we must have $\ker(\varphi) = \langle x^2 + 1 \rangle$ which completes the second proof of the theorem.

Alternative method for computing $\ker(\varphi)$.

If $p \in \ker(\varphi)$, then $p(i) = 0$. Taking the complex conjugates of this equation (using $\overline{z + w} = \bar{z} + \bar{w}$ and $\overline{zw} = \bar{z} \cdot \bar{w}$ for all $z, w \in \mathbb{C}$) we learn that $p(-i) = 0$ as well. As we will see in detail later, $p(i) = 0$ implies $p(x) = (x - i)u(x)$ for some $u \in \mathbb{C}[x]$. Moreover since,

$$0 = p(-i) = -2i \cdot u(-i)$$

we learn that $u(-i) = 0$ and therefore, $u(x) = (x + i)q(x)$ with $q \in \mathbb{C}[x]$. Therefore,

$$p(x) = (x - i)(x + i)q(x) = (x^2 + 1)q(x).$$

It is not too hard to see (use complex conjugation again) that in fact $q \in \mathbb{R}[x]$. Conversely if $p(x) = (x^2 + 1)q(x)$ with $q \in \mathbb{R}[x]$, then $p(i) = 0$. Therefore we have again proved Eq. (11.2). ∎

Lecture 12

Example 12.1. Let $R := \mathbb{Q}[x] / \langle x^2 - 2\rangle$ so that $[x^2] = [2]$ now. Again we take $\mathcal{S} = \{a + bx : a, b \in \mathbb{Q}\}$ and observe that

$$\begin{aligned}[a+bx][c+dx] &= \left[ac + (bc+ad)x + bdx^2\right] \\ &= [ac + (bc+ad)x + bd2] \\ &= [ac + 2bd + (bc+ad)x].\end{aligned}$$

Recalling that, in $\mathbb{Q}\left[\sqrt{2}\right]$, that

$$\left(a + b\sqrt{2}\right)\left(c + d\sqrt{2}\right) = ac + 2bd + (bc+ad)\sqrt{2}$$

it follows that

$$\mathbb{Q}\left[\sqrt{2}\right] \ni a + b\sqrt{2} \to [a+bx] \in \mathbb{Q}[x] / \langle x^2 - 2\rangle$$

is a ring isomorphism.

Example 12.2 (Example 12.1 revisited). Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q}\left[\sqrt{2}\right]$ be the evaluation map, $\varphi(p) = p\left(\sqrt{2}\right)$. Then by the first isomorphism theorem, $\bar{\varphi} : \mathbb{Q}[x] / \ker(\varphi) \to \mathbb{Q}\left[\sqrt{2}\right]$ is an isomorphism of rings. We now claim that

$$\ker(\varphi) = \langle x^2 - 2\rangle. \tag{12.1}$$

Since $x^2 - 2 \in \ker(\varphi)$ we know that $\langle x^2 - 2\rangle \subset \ker(\varphi)$. Conversely, if $p \in \ker(\varphi)$ and $p(x) = q(x)\left(x^2 - 2\right) + r(x)$ for some $r(x) = a + bx$ with $a, b \in \mathbb{Q}$, then

$$0 = p\left(\sqrt{2}\right) = q\left(\sqrt{2}\right) \cdot 0 + r\left(\sqrt{2}\right) = a + b\sqrt{2}.$$

As $\sqrt{2}$ is irrational, this is only possible if $a = b = 0$, i.e. $r(x) = 0$. Thus we have shown $p \in \langle x^2 - 2\rangle$ and therefore Eq. (12.1) is valid.

Example 12.3. Let $I := \langle x^2\rangle = \mathbb{R}[x]x^2 \subset \mathbb{R}[x]$. If $p(x) = a_0 + a_1x + \dots + a_nx^n$, then $p + I = a_0 + a_1x + I$ since $a_2x^2 + \dots + a_nx^n \in I$. Alternatively, we now have $[x^2] = 0$ in $\mathbb{R}[x] / \langle x^2\rangle$, so that

$$[p(x)] = [a_0 + a_1x + \dots + a_nx^n] = [a_0 + a_1x].$$

Moreover $[a_0 + a_1x] = 0$ iff $a_0 = a_1 = 0$, so we may take $\mathcal{S} = \{a_0 + a_1x : a_0, a_1 \in \mathbb{R}\}$ – the polynomials of degree less than or equal to 1. Thus it follows that

$$\mathbb{R}[x] / \langle x^2\rangle = \{(a_0 + a_1x) + I : a_0, a_1 \in \mathbb{R}\} \sim \mathbb{R}^2.$$

This induces a ring multiplication on $\mathbb{R}^2$ determined as follows;

$$\begin{aligned}[a_0 + a_1x][b_0 + b_1x] &= [(a_0 + a_1x)(b_0 + b_1x)] \\ &= \left[a_0b_0 + (a_1b_0 + a_0b_1)x + a_1b_1x^2\right] \\ &= [a_0b_0 + (a_1b_0 + a_0b_1)x].\end{aligned}$$

Thus the multiplication rule on $\mathcal{S}$ should be defined by

$$(a_0 + a_1x)(b_0 + b_1x) = a_0b_0 + (a_1b_0 + a_0b_1)x.$$

Alternatively, if we identify $\mathcal{S}$ with $R := \mathbb{R}^2$ and equip R with the multiplication and addition rules,

$$\begin{aligned}(a_0, a_1) \cdot (b_0, b_1) &= (a_0b_0, a_1b_0 + a_0b_1) \text{ and} \\ (a_0, a_1) + (b_0, b_1) &= (a_0 + b_0, a_1 + b_1),\end{aligned} \tag{12.2}$$

then

$$R \ni (a_0, a_1) \to a_0 + a_1x + I \in \mathbb{R}[x] / \langle x^2\rangle$$

is a ring isomorphism.

An important point to observe for later is that R in Example 12.3 is **not** a field and in fact not even an integral domain. For example, $(0,1)\cdot(0,1) = (0,0) = 0$. Alternatively, notice that $[x] \cdot [x] = [x^2] = 0$, so that $0 \neq [x] \in \mathbb{R}[x] / \langle x^2\rangle$ is a zero divisor.

Example 12.4 (Example 12.3 revisited). We let R be the ring, $\mathbb{R}^2$, with usual addition and the multiplication rule in Eq. (12.2). Let $\varphi : \mathbb{R}[x] \to R$ be the map define by, $\varphi(p) = (p(0), p'(0))$ where $p'(x)$ is the derivative of $p(x)$ computed as usual for polynomials. Then one easily checks that φ is a ring homomorphism. Moreover if $p \in \ker(\varphi)$, then $p(0) = 0$ and therefore $p(x) = xg(x)$ for some polynomial $g(x)$. Since

$$0 = p'(0) = g(0) + 0 \cdot g'(0)$$

it follows that $g(x) = xq(x)$ for some polynomial $q(x)$. Thus $p(x) = x^2 q(x)$. Conversely if $p(x) = x^2 q(x)$, then $p(0) = 0$ and $p'(0) = \left[2xq(x) + x^2 q'(x)\right]_{x=0} = 0$. Therefore we have shown, $\ker(\varphi) = \langle x^2 \rangle$ and so by the first isomorphism theorem, it follows that $\mathbb{R}[x] / \langle x^2 \rangle \ni [p(x)] \to (p(0), p'(0)) \in R$ is a ring isomorphism.

12.1 Higher Order Zeros (Not done in class)

Remark 12.5. Example 12.4 generalizes in the following way. Let $n \in \mathbb{Z}_+$ and $\lambda \in \mathbb{R}$ and define $\varphi : \mathbb{R}[x] \to R := \mathbb{R}^{n+1}$ by

$$\varphi(p) := \left(p(\lambda), p'(\lambda), \ldots, p^{(n)}(\lambda)\right) \in R. \tag{12.3}$$

We wish to define $+$ and $\cdot$ on R so that his map is a homomorphism. Since the derivative operation is linear we should use the ordinary vector addition on $\mathbb{R}^{n+1}$ in which case φ will be an additive group homomorphism. For the multiplication rule we have to use the product rule of differentiation in the following form,

$$(pq)^{(k)}(\lambda) = \sum_{j=0}^{k} \binom{k}{j} p^{(j)}(\lambda)\, q^{(k-j)}(\lambda).$$

Thus if $a = (a_0, \ldots, a_n)$ and $b = (b_0, \ldots, b_n)$, we should define

$$a \cdot b := \left((a \cdot b)_0, \ldots, (a \cdot b)_n\right) \tag{12.4}$$

where

$$(a \cdot b)_k := \sum_{j=0}^{k} \binom{k}{j} a_j \cdot b_{k-j}. \tag{12.5}$$

Theorem 12.6. *Suppose that $R = \mathbb{R}^{n+1}$ with the addition and multiplication operations described in Remark 12.5. Then;*

1. *R is a ring with identity, $1 = (1, 0, \ldots, 0)$.*
2. *$\varphi : \mathbb{R}[x] \to R$ defined in Eq. (12.3) is a ring homomorphism.*
3. $\ker(\varphi) = \left\langle (x-\lambda)^{n+1} \right\rangle = \mathbb{R}[x](x-\lambda)^{n+1}$.

Proof. Item 1. can be proved by a straight forward but tedious verification. However there is a better way! Consider the bijective map,

$$R \ni (a_0, \ldots, a_n) \xrightarrow{\varphi} \left[\sum_{k=0}^{n} \frac{a_k}{k!} x^k\right] := \sum_{k=0}^{n} \frac{a_k}{k!} x^k + \left\langle x^{n+1} \right\rangle \subset \mathbb{R}[x] / \left\langle x^{n+1} \right\rangle.$$

Since,

$$\begin{aligned}\left[\sum_{k=0}^{n} \frac{a_k}{k!} x^k\right] \left[\sum_{l=0}^{n} \frac{b_l}{l!} x^l\right] &= \left[\sum_{k=0}^{2n} \left(\sum_{j=0}^{k} \frac{a_j}{j!} \frac{b_{k-j}}{(k-j)!}\right) x^k\right] \\ &= \left[\sum_{k=0}^{n} \frac{1}{k!} \left(\sum_{j=0}^{k} \binom{k}{j} a_j b_{k-j}\right) x^k\right],\end{aligned}$$

that φ becomes a ring homomorphisms provided we use the multiplication rule in Eqs. (12.4) and (12.5).

Item 2. is easy since we defined the ring multiplication on R so that φ would be a homomorphism.

For item 3. let me only explain the case where $n = 1$ here. If $p \in \ker(\varphi)$, then

$$0 = (0,0) = \varphi(p) = (p(\lambda), p'(\lambda)).$$

Since $p(\lambda) = 0$, we know $p(x) = (x-\lambda) u(x)$ for some $u \in \mathbb{R}[x]$. Differentiating this equation at $x = \lambda$ then implies, $0 = p'(\lambda) = u(\lambda)$ and therefore $u(x) = (x-\lambda) q(x)$ for some $q \in \mathbb{R}[x]$. Therefore $p(x) = (x-\lambda)^2 q(x)$ for some $q \in \mathbb{R}[x]$. Conversely if $p(x) = (x-\lambda)^2 q(x)$, then

$$\varphi(p) = \varphi((x-\lambda))\, \varphi((x-\lambda))\, \varphi(q) = (0,1)(0,1)\, \varphi(q) = (0,0)\, \varphi(q) = 0.$$

Thus we have shown, $\ker(\varphi) = \mathbb{R}[x](x-\lambda)^2$ as claimed when $n = 1$. (We have also shown that $(0,1)$ is a zero divisor in R and hence R is **not** an integral domain.) ■

12.2 More Example of Factor Rings

Example 12.7. Here is another example similar to Example 11.1. In $R := \mathbb{Z}[i] / \langle 3 + i \rangle$, we have $[i] = [-3]$ and therefore $[-1] = [9]$ or equivalently $[10] = 0$. Therefore for $a, b \in \mathbb{Z}$,

$$[a + ib] = [a - 3b] = [(a - 3b) \bmod 10].$$

Thus we should take $\mathcal{S} = \{0, 1, 2, \ldots, 9\}$. If $a, b \in \mathcal{S}$ and $[a] = [b]$, then $[c] = 0$ where $c = (b - a) \bmod 10$. Since $[c] = 0$, we must have

$$c = (3 + i)(a + ib) = (3a - b) + (a + 3b)\, i$$

from which it follows that $a = -3b$ and $3(-3b) - b = -10b = c$. Since $0 \le c \le 9$, this is only possible if $c = 0$ and so as above if $a = b$. Therefore

$$\mathcal{S} \ni a \to [a] = a + \langle 3+i \rangle \in \mathbb{Z}[i] / \langle 3+i \rangle$$

is a bijection. Moreover it is easy to see that thinking of $\mathcal{S}$ as $\mathbb{Z}_{10}$, the above map is in fact a ring isomorphism.

Example 12.8 (Example 12.7 revisited). From Example 8.9 we have seen that $\varphi : \mathbb{Z}[i] \to \mathbb{Z}_{10}$ defined by $\varphi(a+bi) = (a-3b) \bmod 10$ is a ring homomorphism – recall that $3^2 = (-3)^2 = 9 = -1$. In this case,

$$a + ib \in \ker(\varphi) \iff a - 3b = 0 \text{ in } \mathbb{Z}_{10},$$

i.e. $a = 3b + 10k$ for some $k \in \mathbb{Z}$. Therefore,

$$\ker(\varphi) = \{3b + 10k + ib : b, k \in \mathbb{Z}\} = \mathbb{Z}(3+i) + \mathbb{Z} \cdot 10.$$

In particular it follows that $3 + i \in \ker(\varphi)$ and therefore

$$\langle 3+i \rangle \subset \ker \varphi = \mathbb{Z}(3+i) + \mathbb{Z} \cdot 10.$$

Moreover, since $(3-i)(3+i) = 10$, we see that

$$\mathbb{Z}(3+i) + \mathbb{Z} \cdot 10 \subset \mathbb{Z}(3+i) + \mathbb{Z}[i](3+i) = \mathbb{Z}[i](3+i) = \langle 3+i \rangle.$$

Hence we have shown,

$$\langle 3+i \rangle \subset \ker \varphi = \mathbb{Z}(3+i) + \mathbb{Z} \cdot 10 \subset \langle 3+i \rangle$$

and therefore

$$\ker \varphi = \mathbb{Z}(3+i) + \mathbb{Z} \cdot 10 = \langle 3+i \rangle = \mathbb{Z}[i](3+i).$$

Consequently, by the first isomorphism theorem, $\bar{\varphi} : \mathbb{Z}[i]/\langle 3+i \rangle \to \mathbb{Z}_{10}$, given by

$$\bar{\varphi}([a+bi]) = \varphi(a+bi) = (a-3b) \bmod 10$$

is a ring isomorphism. Again, by taking $b = 0$, we see that $\bar{\varphi}^{-1}(a) = [a] = a + \langle 3+i \rangle$ is the inverse isomorphism, compare with Example 12.7.

Theorem 12.9. *Let $\rho \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$ such that $a + ib \neq 0$ and $1 = \gcd(a,b)$. Further let*

$$\mathcal{S} := \mathbb{Z}_{\rho(a^2+b^2)} + i\mathbb{Z}_\rho = \left\{x + iy : x \in \mathbb{Z}_{\rho(a^2+b^2)} \text{ and } y \in \mathbb{Z}_\rho\right\}$$

where $\mathbb{Z}_1 := \{0\}$ and in this case we may take $\mathcal{S} := \mathbb{Z}_{\rho(a^2+b^2)}$. Then the map,

$$\mathcal{S} \ni (x+iy) \xrightarrow{\varphi} [x+iy] \in \mathbb{Z}[i] / \langle \rho(a+ib) \rangle \tag{12.6}$$

is a bijection of sets. If we further assume that $\rho = 1$, then

$$\mathbb{Z}_{(a^2+b^2)} \ni x \to [x] \in \mathbb{Z}[i] / \langle a+ib \rangle \tag{12.7}$$

is an isomorphism of rings.

Proof. The proof is carried out in a number of steps.

1. First observe that
$$\begin{aligned}\langle \rho(a+ib) \rangle &= \{\rho(a+ib)(s+it) : s,t \in \mathbb{Z}\} \\ &= \{\rho[as - bt + i(bs+at)] : s,t \in \mathbb{Z}\}.\end{aligned} \tag{12.8}$$
2. There exists $s, t \in \mathbb{Z}$ such that $bs + at = 1$ and so from Eq. (12.8) it follows that $[\rho i] = [bt - as]$. Therefore every element of $\mathbb{Z}[i] / \langle \rho(a+ib) \rangle$ may be represented in the form $[x+iy]$ where $x \in \mathbb{Z}$ and $y \in \mathbb{Z}_\rho$. Notice that
$$\rho = \min\{\beta \in \mathbb{Z}_+ : \alpha + i\beta \in \langle \rho(a+ib) \rangle \text{ for some } \alpha \in \mathbb{Z}\}.$$
3. If $s, t \in \mathbb{Z}$ such that $bs + at = 0$, then $(s,t) = \lambda(a,-b)$ for some $\lambda \in \mathbb{Q}$. In fact λ can not be a fraction. If it were, since both $s, t \in \mathbb{Z}$, the denominator (in reduced form) of λ would have to divide both a and b and hence $\lambda = \pm 1$ as $\gcd(a,b) = 1$. Thus we have $\lambda \in \mathbb{Z}$.
For such $(s,t) = \lambda(a,-b)$ with $\lambda \in \mathbb{Z}$ we have
$$\rho[as - bt + i(bs+at)] = \lambda\rho\left(a^2+b^2\right).$$
So the smallest positive number this expression can take is $\rho\left(a^2+b^2\right)$ which occurs when $\lambda = 1$.
4. From item 3. it follows that $\left[\rho\left(a^2+b^2\right)\right] = 0$. Combining this observation with item 2. shows that the map, φ, in Eq. (12.6) is onto.
5. The last main thing to prove is that the map φ is one to one. Suppose that $x + iy$ and $x' + iy'$ are in $\mathcal{S}$ with $[x+iy] = [x'+iy']$. This happens iff
$$[x - x' + i(y-y')] = [0] \iff x - x' + i(y-y') \in \langle \rho(a+ib) \rangle. \tag{12.9}$$
Since $|y - y'| < \rho$, it follows form item 2. that if Eq. (12.9) holds then $y - y' = 0$. Since $|x - x'| < \rho\left(a^2+b^2\right)$, it now follows from item 3. that we must have $x - x' = 0$. Thus we have shown $x + iy = x' + iy'$ and hence φ is one to one.
6. The assertion that when $\rho = 1$ the map in Eq. (12.7) is a ring isomorphism is left to the reader.

■

Example 12.10. In this example, we wish to consider, $\mathbb{Z}[x] / \langle 2x-1 \rangle$. In this ring we have

$$[1] = [2x] = [2][x]$$

which suggests that roughly speaking, "$[x] = 1/2$." Thus we might guess that

$$\mathbb{Z}[x] / \langle 2x-1 \rangle \cong \mathbb{Z}[1/2]. \tag{12.10}$$

The general element of $\mathbb{Z}[1/2]$ is a rational number which has a denominator of the form 2^n for some $n \in \mathbb{N}$. In order to try to prove this, let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[1/2]$ be the evaluation map, $\varphi(p) = p(1/2)$. Since $\varphi(\mathbb{Z}[x]) = \mathbb{Z}[1/2]$ to prove Eq. (12.10) we need to show

$$\ker(\varphi) = \langle 2x-1 \rangle . \tag{12.11}$$

On one hand it is clear that $2x-1 \in \ker(\varphi)$ and therefore $\langle 2x-1\rangle \subset \ker(\varphi)$. For the opposite inclusion, suppose that $p \in \ker(\varphi)$, i.e. $p(1/2) = 0$. By the division algorithm, we may write $p(x) = q(x)(x-1/2) + r$ where $r \in \mathbb{Q}$. Since $p(1/2) = 0$ it follows that $r = 0$. Let $g(x) := \frac{1}{2}q(x)$, then $g(x) \in \mathbb{Q}[x]$ satisfies,

$$p(x) = g(x)(2x-1).$$

I claim that $g(x) \in \mathbb{Z}[x]$. To see this look at the expressions,

$$p(x) = \sum_{k=0}^{n} a_k x^k = \left(\sum_{j=0}^{n-1} b_j x^j\right)(2x-1)$$

where $a_k \in \mathbb{Z}$ and $b_k \in \mathbb{Q}$. By looking at the coefficient of the x^k term we learn, $a_k = -b_k + 2b_{j-1}$ with the convention that $b_{-1} = 0 = b_n$. So for $k = 0$ we learn that $b_0 = -a_0 \in \mathbb{Z}$, and for general k, that $b_k = -a_k + 2b_{j-1}$. Thus it follows inductively that $b_k \in \mathbb{Z}$ for all k.

Hence we have shown if $p \in \ker(\varphi)$, then $p \in \langle 2x-1\rangle$, i.e. $\ker(\varphi) \subset \langle 2x-1\rangle$ which completes the proof of Eq. (12.11).

12.3 II. More on the characteristic of a ring

Let R be a ring with 1. Recall: the characteristic of R is the minimum $n > 1$ (if any exist) such that $n \cdot 1 = \overbrace{1 + \cdot + 1}^{n} = 0$. If no such n exists, we call $\operatorname{chr}(R) = 0$.

Theorem 12.11 (Characteristic Theorem). *Let R be a ring with 1. Then $\varphi(a) := a \cdot 1_R$ is a homomorphism from $\mathbb{Z} \to R$ and $\ker\varphi = \langle m\rangle$ where $m = \operatorname{chr}(R)$. Moreover, R contains a copy of $\mathbb{Z}/\langle m\rangle$ as a subring.*

Proof. Since $1_R^2 = 1_R$, we have already seen that $\varphi(a) = a \cdot 1_R$ defines a homomorphism Moreover it is clear that $a \cdot 1_R = 0$ iff $\operatorname{chr}(R)\,|a$, i.e. $\ker(\varphi) = \langle m\rangle$. The remaining statement follows by an application of the first isomorphism theorem; i.e. $\mathbb{Z}/\langle m\rangle \cong \varphi(Z) = \operatorname{Ran}\varphi$. So $\operatorname{Ran}\varphi$ is a subring of R, and it is isomorphic to $\mathbb{Z}/\langle m\rangle$. ■

So the rings $\mathbb{Z}$ and $\mathbb{Z}/\langle m\rangle \cong \mathbb{Z}_m$ are the "simplest" rings in the sense that every ring with 1 has a copy of one of these sitting inside of it.

Example 12.12. Let $m \geq 2$ and

$$R = M_2(\mathbb{Z}_m) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}_m \right\}.$$

Then the homomorphisms above is $\varphi : \mathbb{Z} \to M_2(\mathbb{Z}_m)$ by

$$a \mapsto a \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

$\ker\varphi = \langle m\rangle$, and R has the subring

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a, b, c, d \in \mathbb{Z}_m \right\}$$

which is isomorphic is $\mathbb{Z}_m$.

Example 12.13. If $R = \mathbb{Z}_m$ the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ constructed above is just the natural one $a \mapsto a \bmod m$ that we have been looking at all along and $\operatorname{chr}(\mathbb{Z}_m) = m$.

Example 12.14. If $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Then $\varphi : \mathbb{Z} \to \mathbb{Z}[i], a \mapsto a \cdot 1 = a + 0i$ has kernel $\ker\varphi = \langle 0\rangle$. So $\operatorname{chr}(\mathbb{Z}[i]) = 0$ and $\mathbb{Z}[i]$ has a copy of $\mathbb{Z}/\langle 0\rangle \cong \mathbb{Z}$ inside it, namely $\{a + 0i : a \in \mathbb{Z}\}$.

12.4 Summary

Let us summarize what we know about rings so far and compare this to the group theory of last quarter.

	Group	**Ring**
Definition	G with $\cdot$,associative, identity,multiplicative inverse.	R with $(+,\cdot)$ $\ni (R,+)$ is an abelian group (can add and subtract). Associative, distributive laws $a(b+c)=ab+ac$, $(b+c)a=ba+ca$.
Sub -structure	$H\subset G$ is a subgroup if $h_1h_2^{-1}\in H$ for all $h_1,h_2\in H$, i.e. H is closed under the group operations	$S\subset R$ is a subring if $a-b\in S,\ \ ab\in S$ $\forall\ \ a,b\in S$.
Factor Structure	If $H\lhd G$ is a normal subgroup of G, then $G/H:=\{gH:g\in G\}$ is the factor group of G by H.	If $I\subset R$ is an ideal, then $R/I=\{r+I:r\in R\}$ is the factor ring of R by I.
Homo-morphisms: Functions Preserving Structure	$\varphi:G\to H$ a function between groups, G, and H is a homomorphism if $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)$ for all $g_1,g_2\in G$.	$\varphi:R\to S$ is a function between two rings R and S is a homomorphism if $\varphi(r_1+r_2)=\varphi(r_1)+\varphi(r_2)$ and $\varphi(r_1r_2)=\varphi(r_1)\varphi(r_2)$ for all $r_1,r_2\in R$.

Lecture 13

13.1 Ideals and homomorphisms

Example 13.1. Let $R = \mathbb{Z}$. We have already seen that the ideals of $\mathbb{Z}$ are exactly $\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \mathbb{Z}$, $\langle 2 \rangle, \langle 3 \rangle, \dots$, i.e., every ideal is a principle ideal of the form $\langle m \rangle$ for some $m \geq 0$. We already know that the ideal $\langle m \rangle$ is the kernel of the homomorphism $\mathbb{Z} \to \mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m$.

Theorem 13.2 (Kernels are ideals). *Let R be a ring and $I \subset R$ be an ideal. Then the that map, $\pi : R \to R/I$, defined by*

$$\pi (a) := [a] = a + I \text{ for all } a \in R,$$

is a homomorphism of rings called that ***natural homomorphism.*** *In particular as subset, $S \subset R$ is an ideal iff S is the kernel of some ring homomorphism.*

Proof. We have already seen in Lemma 7.6 that kernels of ring homomorphisms are ideals. We leave it to the reader to verify $\pi : R \to R/I$ is a homomorphism with $\ker \pi = I$. Once this is done, it follows that every ideal is also the kernel of some homomorphism – namely π. ■

Lemma 13.3. *Let $\varphi : R \to \bar{R}$ be a surjective homomorphism of rings and $J \subset R$ be an ideal. Then $\varphi^{-1}(\varphi(J)) = J + \ker(\varphi)$.*

Proof. Unwinding all the definitions implies;

$$\begin{aligned} a \in \varphi^{-1}(\varphi(J)) &\iff \varphi(a) \in \varphi(J) \iff \varphi(a) = \varphi(j) \text{ for some } j \in J \\ &\iff \varphi(a - j) = 0 \text{ for some } j \in J \\ &\iff a - j \in \ker(\varphi) \text{ for some } j \in J \\ &\iff a \in J + \ker(\varphi). \end{aligned}$$

■

Proposition 13.4. *Let $\varphi : R \to \bar{R}$ be a surjective homomorphism of rings and $I := \ker(\varphi)$. Then the two sided ideals of R which contain I are in one to one correspondence with the two sided ideals of $\bar{R}$. The correspondence is given by,*

$$\{J : I \subset J \subset R\} \ni J \to \varphi(J) \subset \bar{R} \text{ and} \tag{13.1}$$
$$\{J : I \subset J \subset R\} \ni \varphi^{-1}(\bar{J}) \longleftarrow \bar{J} \subset \bar{R}. \tag{13.2}$$

Proof. Let us begin by showing that $\varphi(J)$ and $\varphi^{-1}(\bar{J})$ are ideals whenever J and $\bar{J}$ are ideals. First off it is easy to verify that $\varphi(J)$ and $\varphi^{-1}(\bar{J})$ are sub-rings if J and $\bar{J}$ are subrings. Moreover, for $r \in R$, we have

$$\varphi\left(r\varphi^{-1}(\bar{J})\right) = \varphi(r)\,\varphi\left(\varphi^{-1}(\bar{J})\right) = \varphi(r)\,\bar{J} \subset \bar{J}$$

and similarly,

$$\varphi\left(\varphi^{-1}(\bar{J})\,r\right) = \varphi\left(\varphi^{-1}(\bar{J})\right)\varphi(r) = \bar{J}\varphi(r) \subset \bar{J}$$

wherein we have used φ is surjective to conclude that $\varphi\left(\varphi^{-1}(\bar{J})\right) = \bar{J}$. Similarly, if $\bar{r} \in \bar{R}$, there exists $r \in \varphi^{-1}(\{\bar{r}\})$ and therefore,

$$\begin{aligned} \bar{r}\varphi(J) &= \varphi(r)\,\varphi(J) = \varphi(rJ) \subset \varphi(J) \text{ and} \\ \varphi(J)\,\bar{r} &= \varphi(J)\,\varphi(r) = \varphi(Jr) \subset \varphi(J) \end{aligned}$$

which shows that $\varphi(J)$ is an ideal as well.

Lastly we show that the maps in Eqs. (13.1) and (13.2) are inverses to one another. Indeed,

$$\begin{aligned} \varphi\left(\varphi^{-1}(\bar{J})\right) &= \bar{J} \text{ and} \\ \varphi^{-1}(\varphi(J)) &= J + I = J. \end{aligned}$$

In the first line we have used that fact that φ is surjective while in the second we used Lemma 13.3 and the assumption that $I = \ker(\varphi) \subset J$ so that $I + J = J$. ■

Example 13.5. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ be the evaluation homomorphism, $\varphi(f(x)) = f(0)$ so that

$$\ker(\varphi) = \langle x \rangle = \{f(x) \in \mathbb{Z}[x] : f(0) = 0\}.$$

For any $m \in \mathbb{Z}$, $\langle m \rangle \subset \mathbb{Z}$ is an ideal and therefore,

$$\varphi^{-1}(\langle m \rangle) = \{f(x) \in \mathbb{Z}[x] : f(0) \in \langle m \rangle\}$$

is an ideal in $\mathbb{Z}[x]$ which contains $\langle x \rangle$. In fact this is the list of all ideals of $\mathbb{Z}[x]$ which contain $\langle x \rangle = \varphi^{-1}(\{0\})$.

Corollary 13.6. *If $I \subset R$ is an ideal than the ideals of R/I are in one to one correspondence with the ideals of R containing I. The correspondence is given by $J \subset R$ with $I \subset J$ is sent to $\pi(J) = \{[a] = a + I : a \in J\}$.*

Example 13.7. Let us find all of the ideals of $\mathbb{Z}/\langle 10\rangle$. Since that ideals of $\mathbb{Z}$ containing $\langle 10\rangle$ are;

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}, \ \langle 2\rangle = 0, \pm 2, \pm 4, \dots\},$$
$$\langle 5\rangle = \{0, \pm 5, \pm 10, \dots\}, \text{ and } \langle 10\rangle = \{0, \pm 10, \pm 20, \dots\},$$

it follows by Corollary 13.6 that the ideals of $\mathbb{Z}/\langle 10\rangle$ are given by

$$\begin{aligned} \mathbb{Z}/\langle 10\rangle &= \{0, 1, 2, \dots, 9\} + \langle 10\rangle, \\ \langle 2\rangle/\langle 10\rangle &= \{0, 2, 4, 6, 8\} + \langle 10\rangle, \\ \langle 5\rangle/\langle 10\rangle &= \{0, 5\} + \langle 10\rangle, \text{ and} \\ \langle 10\rangle/\langle 10\rangle &= \{0\} + \langle 10\rangle. \end{aligned}$$

13.2 Maximal and Prime Ideals

Let R be a ring, and I an ideal. How do we tell if R/I has properties we like? For example, when is R/I a domain or when is R/I a field? It turns out that this has nothing to do with R itself but rather only depends on properties of the ideal, I. We explore these connections in the context where R is a commutative ring with $1 \in R$.

Definition 13.8. *Let R be a commutative ring with identity 1. An ideal I is called* ***prime*** *if given any $a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$. An ideal I is called* ***maximal*** *if given an ideal J with $I \subset J \subset R$ either $I = J$ or $J = R$.*

Example 13.9. In $\mathbb{Z}$, the ideal $\langle m\rangle$ is neither prime nor maximal when m is composite. For example, $\langle 6\rangle$ is not prime. We see that $2 \cdot 3 = 6 \in \langle 6\rangle$, but $2 \notin \langle 6\rangle$, and $3 \notin \langle 6\rangle$. Moreover $\langle 6\rangle \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}$ and $\langle 6\rangle \subsetneq \langle 3\rangle \subsetneq \mathbb{Z}$ which shows that $\langle 6\rangle$ is not prime. On the other hand, if p is prime, then the ideal $\langle p\rangle$ is both prime and maximal. Let us also observe that $\langle 0\rangle = \{0\}$ is prime, but not maximal. To see that it is not maximal simply observe, for example, that $\langle 0\rangle \subsetneq \langle 2\rangle \subsetneq \mathbb{Z}$. The fact that $\langle 0\rangle$ is prime is equivalent to the statement that $\mathbb{Z}$ is an integral domain, see the next lemma.

Example 13.10. Consider the ideal, $I := \langle x\rangle \subset \mathbb{Z}[x]$. This ideal is prime. Indeed, if $p, q \in \mathbb{Z}[x]$, then

$$\begin{aligned} p(x)\, q(x) \in I &\implies p(0)\, q(0) = 0 \\ &\implies p(0) = 0 \text{ or } q(0) = 0 \implies p(x) \in I \text{ or } q(x) \in I. \end{aligned}$$

On the other hand, because of Example 13.5 we know that $\langle x\rangle$ is not a maximal ideal.

Lecture 14

Lemma 14.1. *Let R be a commutative ring with identity $1 = 1_R$. Then R is an integral domain iff $\langle 0 \rangle = \{0\}$ is a prime ideal and R is a field iff $\langle 0 \rangle = \{0\}$ is a maximal ideal.*

Proof. Suppose that $a, b \in R$. Then $ab \in \langle 0 \rangle$ iff $ab = 0$. If $\langle 0 \rangle$ is a prime ideal then $a \in \langle 0 \rangle$ or $b \in \langle 0 \rangle$, i.e. either $a = 0$ or $b = 0$. This shows that R is an integral domain. Similarly if R is an integral domain and $ab \in \langle 0 \rangle$, then $ab = 0$ and hence either $a = 0$ or $b = 0$, i.e. either $a \in \langle 0 \rangle$ or $b \in \langle 0 \rangle$. Thus $\langle 0 \rangle$ is a prime ideal.

You are asked to prove on your homework that R is a field iff the only ideals of R are $\{0\}$ and R. Now $\{0\}$ is maximal iff the only other ideal of R is R itself. ■

Theorem 14.2. *Suppose that R and $\bar{R}$ are commutative rings with identities and $\varphi : R \to \bar{R}$ is a surjective homomorphism. Then an ideal, $J \subset R$ such that* $\ker(\varphi) \subset J$ *is prime (maximal) iff $\varphi(J)$ is prime (maximal) in $\bar{R}$. Similarly, an ideal $\bar{J} \subset \bar{R}$ is prime (maximal) iff $\varphi^{-1}(\bar{J})$ is prime (maximal) in R.*

Proof. We begin by proving the statements referring to J. In what follows below J will always be an ideal of R containing $\ker(\varphi)$.

1. Suppose that $J \subset R$ is prime and let $\bar{a} = \varphi(a)$ and $\bar{b} = \varphi(b)$ are generic elements of $\bar{R}$. Then $\bar{a}\bar{b} \in \varphi(J)$ iff $\varphi(a)\varphi(b) = \varphi(j)$ for some $j \in J$ which happens iff $ab - j \in \ker(\varphi)$, i.e. $ab \in J + \ker(\varphi) = J$. Since J is prime it follows that either a or $b \in J$ and therefore either $\bar{a}$ or $\bar{b}$ in $\varphi(J)$.
Now suppose that $\varphi(J)$ is prime. If $a, b \in R$ such that $ab \in J$, then $\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(J)$. Since $\varphi(J)$ is prime it follows that either $\varphi(a)$ or $\varphi(b)$ is in $\varphi(J)$, i.e. either a or $b \in \varphi^{-1}(\varphi(J)) = J + \ker(\varphi) = J$.
2. If $J \subset R$ is not a maximal ideal then there exists an ideal K such that $J \subsetneq K \subsetneq R$. Since $\varphi^{-1}(\varphi(J)) = J$, $\varphi^{-1}(\varphi(K)) = K$, $\varphi^{-1}(\bar{R}) = R$, it follows that $\varphi(J) \subsetneq \varphi(K) \subsetneq \bar{R}$ which shows $\varphi(J)$ is not maximal. Conversely if $\varphi(J)$ is not maximal, there exists an ideal, $\bar{K}$ of $\bar{R}$, such that $\varphi(J) \subsetneq \bar{K} \subsetneq \bar{R}$. Then $K := \varphi^{-1}(\bar{K})$ is an ideal of R that $J \subset K \subset R$. Since $\varphi(J) \subsetneq \bar{K} = \varphi(K) \subsetneq \bar{R}$, it follows that $J \subsetneq K \subsetneq R$ and hence J is not maximal.

The statements referring to $\bar{J}$ now follow from what we have already proved. Indeed, let $\bar{J} \subset \bar{R}$ be an ideal and $J := \varphi^{-1}(\bar{J})$ which is an ideal of R containing $\ker(\varphi)$. By what we have already proved we know that $\varphi^{-1}(\bar{J}) = J$ is prime (maximal) in R iff $\bar{J} = \varphi(\varphi^{-1}(\bar{J})) = \varphi(J)$ is prime (maximal) in $\bar{R}$. ■

The following theorem is now an easy corollary of Lemma 14.1 and Theorem 14.2.

Theorem 14.3. *Let R be commutative with 1, I a prime ideal. Then*

1. *R/I is an integral domain $\Leftrightarrow$ I is a prime.*
2. *R/I is a field $\Leftrightarrow$ I is maximal.*

Proof. Easy Proof. As usual we will write $[a]$ for $a + I$ and recall from your homework that R/I is a commutative ring with identity, $[1] = 1 + I$. Let $\pi : R \to R/I$ be the natural homomorphism, $\pi(a) = [a] = a + I$. Then $I = \ker(\pi) = \pi^{-1}(\{0\})$. Therefore, by Theorem 14.2, $I \subset R$ is prime (maximal) iff $\{0\} \subset R/I$ is prime (maximal). But by Lemma 14.1 we know that $\{0\} \subset R/I$ is prime iff R/I is an integral domain and $\{0\} \subset R/I$ is maximal iff R/I is a field.

Second Proof. To help the reader understand this theorem better, let us also give a second more direct proof of the theorem.

1. Suppose I is prime and $[ab] = [a][b] = [0]$ in R/I, then $ab \in I$. Since I is prime it follows that $a \in I$ or $b \in I$, i.e. $[a] = 0$ or $[b] = 0$. Therefore R/I has no zero divisors, i.e. R/I is an integral domain.
Conversely, if I is not prime there exists $a, b \in R \setminus I$ with $ab \in I$. Therefore $[a] \neq 0 \neq [b]$ while $[a][b] = [ab] = 0$ which shows that R/I has zero divisors and hence is not an integral domain.
2. Suppose that I is maximal and let $0 \neq [a] \in R/I$ so that $a \in R$ but $a \notin I$. Let J be the ideal generated by a and I, i.e.
$$J := Ra + I = \{ra + b : r \in R, b \in I\}.$$
(You should check that J is an ideal.) Since $a \in J$ it follows that $I \subsetneq J$ and since I was maximal we may conclude that $J = R$. In particular $1 \in J$ and hence there exists $r \in R$ and $b \in I$ such that $1 = ra + b$. Therefore, $1 = [1] = [ra] = [r] \cdot [a]$ which shows $[a]^{-1}$ exists and is equal to $[r]$. Therefore $U(R/I) = (R/I) \setminus \{0\}$ which shows R/I is a field.
Conversely if I is not maximal, then there exists another ideal, J, of R such that $I \subsetneq J \subsetneq R$. Let $b \in J \setminus I$ so that $[b] = b + I \neq 0$. If $[b]^{-1}$ exists, then

there exist $a \in R$ such that $[a][b] = 1 = [1]$, i.e. $i := ab - 1 \in I$. Solving for 1 gives,

$$1 = i + ab \in I + J \subset J.$$

This however contradicts the fact that J is proper since $R = R\cdot 1 \subset RJ = J$. Thus $[b]$ is not invertible for all $b \in J \setminus I$.

■

Corollary 14.4. *In a commutative ring R with 1, every maximal ideal is also a prime ideal.*

Proof. First Proof. This follows from the Theorem 14.3 since a field is always an integral domain.

Second Proof. Suppose I is a maximal ideal that $a \notin I$ and let $J := I + Ra = J + \langle a \rangle$. Then J is an ideal in R which properly contains I and therefore we must have $J = R$. Hence it follows that $1 = ra + i$ for some $r \in R$ and $i \in I$. So if $ab \in I$ then

$$b = rab + ib \in I$$

showing I is a prime ideal. ■

Example 14.5 (Example 13.9 revisited). Since $\mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m$ and $\mathbb{Z}_m$ is an integral domain (field) iff m is prime, we see that the following are equivalent,

1. m is prime,
2. $\langle m \rangle$ is a prime ideal of $\mathbb{Z}$, and
3. $\langle m \rangle$ is a maximal ideal of $\mathbb{Z}$.

Example 14.6. In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $I = \{0, 3\}$ is a maximal ideal. To see this let $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_3$ be the homomorphism, $\varphi(x) = x \bmod 3$. Then $\ker(\varphi) = I$ and since $\mathbb{Z}_3$ is a field it follows that $\langle 0 \rangle$ is a maximal ideal and hence $\varphi^{-1}(\{0\}) = \ker(\varphi)$ is a maximal ideal.

Example 14.7. In $\mathbb{R}[x]$, $\langle x \rangle$ is maximal since $\mathbb{R}[x] / \langle x \rangle \cong \mathbb{R}$. Notice also that $\langle 0 \rangle$ is prime since $\mathbb{R}[x]$ is an integral domain but not maximal since $\mathbb{R}[x]$ is not a field.

Example 14.8. $\langle 2 - i \rangle$ is maximal inside of $\mathbb{Z}[i]$. This is hard to see without our earlier result that $\mathbb{Z}[i]/\langle 2 - i \rangle \simeq \mathbb{Z}_5$, which is a field.

Example 14.9. Let $I := \langle 2, x \rangle = \mathbb{Z}[x] \cdot 2 + \mathbb{Z}[x] \cdot x$ – an ideal of $\mathbb{Z}[x]$. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ be the evaluation homomorphism, $\varphi(p(x)) = p(0)$ with $\ker\varphi = \langle x \rangle$. Notice that $\ker\varphi \subset I$ and that $\varphi(I) = 2\mathbb{Z} = \langle 2 \rangle$. Since $\langle 2 \rangle$ is maximal in $\mathbb{Z}$ we know that $I = \langle 2, x \rangle$ is a maximal ideal of $\mathbb{Z}[x]$. In fact for any prime, $p \in \mathbb{N}$, the same argument shows that $\langle p, x \rangle$ is a maximal ideal of $\mathbb{Z}[x]$ and these are precisely all of the maximal ideals of $\mathbb{Z}[x]$ which contain $\langle x \rangle$.

Example 14.10. $\langle x \rangle \subset \mathbb{Z}[x]$ is a prime ideal which is not maximal. Indeed from the previous example, $\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$ which implies $\langle x \rangle$ is not maximal. To see that it is prime observe that $\mathbb{Z}[x] / \langle x \rangle \cong \mathbb{Z}$ is an integral domain. Moreover since $\mathbb{Z}$ is not a field it again follows that $\langle x \rangle$ is not a maximal ideal.

Alternative 1. Observe that $\varphi(\langle x \rangle) = \{0\}$ and $\{0\}$ is prime but not maximal in $\mathbb{Z}$.

Alternative 2. If $f \in \mathbb{Z}[x]$, we have $f(x) = xq(x) + a_0$ and using $[x] = 0 = [2]$ we find

$$[f(x)] = [x][q(x)] + [a_0] = [a_0 \bmod 2].$$

Moreover if $a, b \in \mathbb{Z}_2$ and $[a] = [b]$, then $a - b \in \langle 2, x \rangle$ which is only possible if $a - b = 0$. Thus it follows that we may take $\mathcal{S} = \mathbb{Z}_2$. We may now work as we have done many times before to see that $\mathbb{Z}[x] / \langle 2, x \rangle \cong \mathbb{Z}_2$.

Definition 14.11 (Principle ideal domains). *A **principle ideal domain** (PID for short) is an integral domain, R, such that every ideal $I \subset R$ is a principle ideal.*

Example 14.12. $\mathbb{Z}$ and $\mathbb{Z}_m$ for all $m \in \mathbb{Z}_+$ are principle ideal domains. We will also see later that $F[x]$ is a principle ideal domain for every field F.

Example 14.13. In this example we show that $\mathbb{Z}[x]$ is **not** a principle ideal domain. For example, consider that ideal generated by $\langle 2, x \rangle$, i.e.

$$\begin{aligned} \langle 2, x \rangle &= \mathbb{Z}[x] \cdot 2 + \mathbb{Z}[x] \cdot x \\ &= \{2a + xq(x) : a \in \mathbb{Z} \text{ and } q(x) \in \mathbb{Z}[x]\} \qquad (14.1) \\ &= \{f(x) \in \mathbb{Z}[x] : f(0) \in \langle 2 \rangle\}. \qquad (14.2) \end{aligned}$$

If $\langle 2, x \rangle = \langle p(x) \rangle$ for some $p \in \mathbb{Z}[x]$, then $2 = q(x)p(x)$ for some $q(x) \in \mathbb{Z}[x]$. However, this is only possible if both $q(x)$ and $p(x)$ are constant polynomials in which case we must have $p(x) = a_0 \in \{\pm 1, \pm 2\}$. We can rule out $a_0 = \pm 1$ since $\langle 2, x \rangle$ is a proper ideal and hence we may assume that $p(x) = 2$. Noting that $x \notin \langle 2 \rangle$ we learn that $\langle 2 \rangle \subsetneqq \langle 2, x \rangle$ and therefore $\langle 2, x \rangle$ is not a principle ideal in $\mathbb{Z}[x]$.

Lecture 15

- We first went over Quiz #4 in class.

Lemma 15.1. *Suppose that R is an integral domain and $a, b \in R$ with $a \neq 0 \neq b$. Then $\langle a \rangle = \langle b \rangle$ iff a and b are* ***associates****, i.e. $a = ub$ for some $u \in U(R)$.*

Proof. If $\langle a \rangle = \langle b \rangle$ then $a \in \langle b \rangle$ and $b \in \langle a \rangle$ and therefore there exists $u_1, u_2 \in R$ such that $a = u_1 b$ and $b = u_2 a$. Thus we may conclude that $b = u_2 u_1 b$ and hence by cancellation that $u_2 u_1 = 1$. This shows that $a = ub$ with $u = u_1 \in U(R)$. Conversely if $a = ub$ with $u \in U(R)$ then $a \in \langle b \rangle$ and $b \in \langle a \rangle$ since $b = u^{-1} a$. Therefore, $\langle a \rangle \subset \langle b \rangle$ and $\langle b \rangle \subset \langle a \rangle$, i.e. $\langle a \rangle = \langle b \rangle$. ■

Proposition 15.2 (maximal $\iff$ prime in PIDs). *If R is a principle ideal domain and $I \subset R$ be a non-zero ideal. Then I is maximal iff I is prime.*

Proof. By Corollary 14.4, we know in general that maximal ideals are prime ideals. So we need only show that if I is a prime ideal then I is a maximal ideal. Suppose that $I = \langle a \rangle \subset R$ (with $a \neq 0$) is a prime ideal and $J = \langle b \rangle$ is another ideal such that $I \subset J$. We will finish the proof by showing either $J = I$ or $J = R$.

As $a \in \langle b \rangle$, we have $a = bc$ for some $c \in R$. Since $bc \in I = \langle a \rangle$ and I is prime, we must have either $b \in \langle a \rangle$ or $c \in \langle a \rangle$. Case 1: if $b \in \langle a \rangle$, then $J = \langle b \rangle \subset \langle a \rangle = I$ and hence $J = I$. Case 2: if $c \in \langle a \rangle$, then $c = au$ for some $u \in R$ and we then have $a = bc = bau$. Cancelling a (here is where we use $a \neq 0$) from this equation shows that $1 = bu$ and therefore b and 1 are associates and so, by Lemma[1] 15.1, $J = \langle 1 \rangle = R$. ■

15.1 The rest this section was not covered in class

Lemma 15.3. *Suppose that R_1 and R_2 are two commutative rings with identities.. Then every ideal, $J \subset R_1 \oplus R_2$, is of the form $J = I_1 \oplus I_2$ where I_1 and I_2 are ideals of R_1 and R_2 respectively.*

Proof. It is easy to check that $J := I_1 \oplus I_2 \subset R_1 \oplus R_2$ is an ideal whenever I_1 and I_2 are ideals of R_1 and R_2 respectively. So let us concentrate on the converse assertion.

Suppose that $J \subset R_1 \oplus R_2$. If $(a, b) \in J$, then $(a, 0) = (1, 0)(a, b)$ and $(0, b) = (0, 1)(a, b)$ are in J. It is now a simple matter to check that

$$I_1 := \{a \in R_1 : (a, 0) \in J\} \text{ and } I_1 := \{b \in R_2 : (0, b) \in J\}$$

are ideals of R_1 and R_2 respectively. If $a \in I_1$ and $b \in I_2$, then $(a, b) = (a, 0) + (0, b) \in J$ showing $I_1 \oplus I_2 \subset J$. Similarly if $(a, b) \in J$, then as noted above $a \in I_1$ and $b \in I_2$ which implies $J \subset I_1 \oplus I_2$. ■

Corollary 15.4. *Let R_1, R_2, be as in Lemma 15.3. Then the maximal ideals of $R_1 \oplus R_2$ are of the form $J = I_1 \oplus R_2$ or $J = R_1 \oplus I_2$ where I_1 is a maximal ideal of R_1 and I_2 is a maximal ideal of R_2.*

Example 15.5 (Book problem 14.30). Find the maximal ideals, I, in $R := \mathbb{Z}_8 \oplus \mathbb{Z}_{30}$ and for each maximal ideal find size of the field, R/I. The only maximal ideal of $\mathbb{Z}_8$ is $\langle 2 \rangle$ and the maximal ideals of $\mathbb{Z}_{30}$ are $\langle 2 \rangle$, $\langle 3 \rangle$, and $\langle 5 \rangle$. Thus the maximal ideals of R are

$$\langle 2 \rangle \oplus \mathbb{Z}_{30}, \quad \mathbb{Z}_8 \oplus \langle 2 \rangle, \quad \mathbb{Z}_8 \oplus \langle 3 \rangle, \quad \text{and } \mathbb{Z}_8 \oplus \langle 5 \rangle.$$

The respective fields have size, by Lagrange's theorem or other means, $2 = 8/\frac{8}{\gcd(2,8)}$, $2 = 30/\frac{30}{\gcd(2,30)}$, $3 = 30/\frac{30}{\gcd(3,30)}$, and $5 = 30/\gcd(5, 30)$.

[1] More directly, $1 = bu$ implies b^{-1} exists and therefore $1 = b^{-1} b \in \langle b \rangle = J$ and hence that $J = R$.

Lecture 16

16.1 The Degree of a Polynomial

Recall the following definition of being a polynomial.

Definition 16.1. *Let R be any commutative ring with identity. The polynomial ring $R[x]$ is defined to be*

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : a_i \in R \text{ and } n \geq 0\}$$

equipped with the usual rules for addition and multiplication of polynomials.

Recall that the multiplicative identity in $R[x]$ is 1, and the additive identity is 0.

Notation 16.2 *Suppose that*

$$f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$$

is a polynomial with $a_n \neq 0$. The we say a_n is the ***leading coefficient*** *and f has* ***degree*** *n, written $\deg(f) = n$. (It is convenient to use the convention that $\deg(0) = -\infty$.) If $a_n = 1$, then f is called* ***monic.*** *When $\deg f = 0$, i.e. $f = a_0$, we say f is a* ***constant*** *polynomial.*

Example 16.3. In $\mathbb{C}[x]$, $\deg(4x^2 + (i+3)x + 5) = 2$. The coefficient of the largest power of x is called the leading coefficient. The leading coefficient of $4x^2 + (i+3)x + 5$ is 4. The polynomial $4x^2 + (i+3)x + 5$ is not monic while $g = x^2 + 6$ is monic. $f = 5$ is constant, but $g = x + 5$ is not.

Example 16.4. Let $R = \mathbb{Z}_6 = \{0, 1, \ldots, 5\}$,

$$f = x^2 + 5, \quad g = 2x + 1, \quad \text{and } h = 3x.$$

Then

$$\begin{aligned} fg &= (2x^3 + x^2 + 10x + 5) = 2x^3 + x^2 + 4x + 5, \\ f + g &= x^2 + 2x + 6 = x^2 + 2x, \text{ and} \\ gh &= 6x^2 + 3x = 3x. \end{aligned}$$

In this example, $\deg f = 2$, $\deg g = 1$, $\deg h = 1$, and $\deg(gh) = 1\,(\neq 2)$. So it is not always true in a polynomial ring that $\deg(fg) = \deg g + \deg h$. Let us compute the "values" of $g(x)$;

x	0	1	2	3	4	5
$g(x)$	0	3	0	3	0	3

.

Thus we see that $\deg(g) = 1$ yet $g(x)$ has three roots over $\mathbb{Z}_6$.

Theorem 16.5. *Let R be an integral domain. Then for any $f, g \in R[x]$,*

$$\deg(fg) = \deg(f) + \deg(g),$$

and $R[x]$ is an integral domain.

Proof. If $f = 0$ then $fg = 0$ and we will have $\deg(fg) = -\infty$ and $\deg(f) + \deg(g) = -\infty + \deg(g) = -\infty$. So we may now assume that f and g are non-zero polynomials which we write as,

$$\begin{aligned} f &= a_n x^n + \cdots + a_1 x + a_0, \text{ and} \\ g &= b_m x^n + \cdots + b_1 x + b_0 \end{aligned}$$

with $a_i, b_i \in R$, $a_n \neq 0$, and $b_m \neq 0$. Then $\deg f = n$ and $\deg g = m$. So

$$fg = a_n b_m x^{n+m} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0,$$

and $a_n b_m \neq 0$ so that fg is not the zero polynomial and $\deg(fg) = m + n = \deg f + \deg g$. ■

Lemma 16.6. *If R is an integral domain, then $U(R[x]) = U(R)$. In particular if $R = F$ is a field and $F^\times := F \setminus \{0\}$, then $U(F[x]) = F^\times$.*

Proof. If $p(x) \in U(R[x])$ then there exists $q(x) \in R[x]$ such that $p(x)q(x) = 1$. Therefore, $0 = \deg(p) + \deg(q)$, showing $\deg(p) = 0 = \deg(q)$. Thus $p(x) = p_0 \in R$ and p_0 is invertible in $R[x]$ iff it is invertible in R because we have seen above that $\deg(q) = 0$ where $q(x)$ is the inverse to $p(x) = p_0$. ■

16.2 The evaluation homomorphism (review)

Theorem 16.7 (Evaluation homomorphism). *Let R be a subring of a commutative ring, $\bar{R}$, and $t \in \bar{R}$. Then there exists a ring homomorphism, $\varphi_t : R[x] \to \bar{R}$ such that*

$$\varphi_t(p) = \sum_{k=0}^{n} a_k t^k \text{ when } p(x) = \sum_{k=0}^{n} a_k x^k \in R[x].$$

We will usually simply write $p(t)$ for $\varphi_t(p)$.

Proof. Let $q(x) = \sum_{l=0}^{n} b_l x^l$, then

$$\begin{aligned}\varphi_t(p+q) &= \varphi_t\left(\sum_{l=0}^{n}(a_l+b_l)x^l\right) = \sum_{l=0}^{n}(a_l+b_l)t^l \\ &= \sum_{l=0}^{n}\left(a_l t^l + b_l t^l\right) = \sum_{l=0}^{n} a_l t^l + \sum_{l=0}^{n} b_l t^l \\ &= \varphi_t(p(x)) + \varphi_t(q(x)).\end{aligned}$$

Similarly,

$$\begin{aligned}\varphi_t(pq) &= \varphi_t\left(\sum_m\left(\sum_{l+k=m} a_l b_k\right)x^m\right) \\ &= \sum_m\left(\sum_{l+k=m} a_l b_k\right)t^m = \sum_m\left(\sum_{l+k=m} a_l b_k t^m\right) \\ &= \sum_m\left(\sum_{l+k=m} a_l t^l b_k t^k\right) = \sum_{l,k} a_l t^l b_k t^k \\ &= \left(\sum_l a_l t^l\right)\left(\sum_k b_k t^k\right) = \varphi_t(p)\cdot\varphi_t(q).\end{aligned}$$

The point is that the multiplication and addition rules for polynomials was chosen precisely so as to make this theorem true. ■

Example 16.8. Suppose that $\varphi := \varphi_1 : \mathbb{R}[x] \to \mathbb{R}$ is the evaluation homomorphism, $\varphi(p) = p(1)$. Then

$$\begin{aligned}\varphi(fg) &= fg(1) = f(1)g(1) \text{ and} \\ \varphi(f+g) &= [f+g](1) = f(1)+g(1).\end{aligned}$$

For example suppose that

$$f = x^2+5 \text{ and } g = 2x^3-5x+2.$$

Then

$$\begin{aligned}f+g &= 2x^3+x^2-5x+7, \\ fg &= 2x^5+5x^3+2x^2-25x+10, \\ f(1) &= 6, \quad g(1) = -1,\end{aligned}$$

and so

$$\begin{aligned}(f+g)(1) &= 5 = f(1)+g(1) \text{ and} \\ (fg)(1) &= -6 = f(1)\cdot g(1).\end{aligned}$$

Example 16.9 (Evaluation example). Suppose that $R = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$, $a = 3$, and $\varphi : R[x] \to R$ is the evaluation map, $f \mapsto f(3)$. For example, if $f = 3x^2+5x+2$, and $g = x+3$, then

$$\begin{aligned}\varphi(f) &= f(3) = 3(3)^2+5(3)+2 = 44 = 2 \text{ and} \\ \varphi(g) &= g(3) = 3+3 = 6 = 0,\end{aligned}$$

from which it follows that $f \notin \ker(\varphi)$ while $g \in \ker(\varphi)$.

Example 16.10. Suppose that $\lambda \in \mathbb{R}$ and $\varphi = \mathrm{eval}_\lambda : \mathbb{R}[x] \to \mathbb{R}$, i.e. $\varphi(p) = p(\lambda)$. Then $p \in \ker\varphi$ iff $p(\lambda) = 0$ which happens (as we will see shortly) iff $p(x) = (x-\lambda)q(x)$ for some $q \in \mathbb{R}[x]$. Therefore,

$$\ker(\varphi) = \langle x-\lambda\rangle = \mathbb{R}[x](x-\lambda)$$

for this homomorphism.

16.3 The Division Algorithm

Definition 16.11. *Let R be an integral domain and $f, g \in R[x]$. We say that g **divides** f if $f = kg$ for some $k \in R[x]$. We also say that g is a **factor** of f.*

Example 16.12. In $\mathbb{Z}[x]$, $(2x-4)$ does not divide $\left(x^2-4\right)$. Indeed, if it did then

$$x^2-4 = (a+bx)(2x-4) = -4a+(2a-4b)x+2bx^2$$

which would imply $2b = 1$ which is impossible in $\mathbb{Z}$. On the other hand, working in $\mathbb{Q}[x]$, we have

$$x^2-4 = (x-2)(x+2) = (2x-4)\left(\frac{1}{2}x+1\right)$$

which shows that $(2x-4)$ is a factor of x^2-4 in $\mathbb{Q}[x]$.

Theorem 16.13 (Division Algorithm). *Let $F[x]$ be a polynomial ring where F is a field. Given $f, g \in F[x]$ both nonzero, there exists a unique $q, r \in F[x]$ with $f = qg + r$ such that either $r = 0$ or $\deg r < \deg g$. (We will give the proof of this theorem later.)*

Interpretation. We are dividing f by g and so g **goes into** f, q **times with remainder** r. This is really high school polynomial division which we will discuss in more detail a bit later. In the sequel we will sometimes denote the remainder, r by $f \bmod g$.

Example 16.14. Let $f := 3x^3 + 5$ and $g = 2x + 3$ in $\mathbb{Q}[x]$, then

$$\begin{array}{r|l}
 & \tfrac{3}{2}x^2 - \tfrac{9}{4}x + \tfrac{27}{8} \\ \hline
2x+3 & 3x^3 \qquad\qquad\qquad + 5 \\
 & \underline{-3x^3 - \tfrac{9}{2}x^2} \\
 & \quad - \tfrac{9}{2}x^2 \\
 & \quad \underline{\tfrac{9}{2}x^2 + \tfrac{27}{4}x} \\
 & \qquad \tfrac{27}{4}x + 5 \\
 & \qquad \underline{-\tfrac{27}{4}x - \tfrac{81}{8}} \\
 & \qquad\qquad -\tfrac{41}{8}
\end{array}$$

which shows,

$$3x^3 + 5 = \left(\frac{3}{2}x^2 - \frac{9}{4}x + \frac{27}{8}\right)(2x+3) + \left(-\frac{41}{8}\right)$$

so that

$$q(x) = \left(\frac{3}{2}x^2 - \frac{9}{4}x + \frac{27}{8}\right) \text{ and } r(x) = -\frac{41}{8}$$

in this example.

Example 16.15. Consider $f(x) = x^2 + x + 2$ and $g(x) = 2x + 1$ inside of $\mathbb{Z}_3[x]$. Then, using $2 \cdot 2 = 4 \bmod 3 = 1$, we find

$$\begin{array}{r|l}
 & 2x - 2 \\ \hline
2x+1 & x^2 + x + 2 \\
 & \underline{x^2 + 2x} \\
 & \quad -x + 2 \\
 & \quad \underline{-x - 2} \\
 & \qquad 4 = 1
\end{array},$$

which implies

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

Example 16.16 (Example 16.15). Here is alternate way to do the last example. First use the division algorithm over $\mathbb{Q}$ to find;

$$\begin{array}{r|l}
 & \tfrac{1}{2}x + \tfrac{1}{4}, \\ \hline
2x+1 & x^2 + x + 2 \\
 & \underline{-x^2 - \tfrac{1}{2}x} \\
 & \quad \tfrac{1}{2}x + 2 \\
 & \quad \underline{-\tfrac{1}{2}x - \tfrac{1}{4}} \\
 & \qquad \tfrac{7}{4}
\end{array}$$

that is over $\mathbb{Q}$ we have

$$x^2 + x + 2 = \left(\frac{1}{2}x + \frac{1}{4}\right)(2x+1) + 7/4.$$

Multiplying this equation through by 4 gives,

$$4\left(x^2 + x + 2\right) = (2x+1)(2x+1) + 7$$

and then apply the "mod 3 homomorphism" to the coefficients implies,

$$x^2 + x + 2 = (2x+1)(2x+1) + 1$$

which is the result above again.

Example 16.17. Let $f(x) = 2x^3$ and $g(x) = ix^2 + 5x + 2$ in $\mathbb{C}[x]$, then

$$\begin{array}{r|l}
 & -2ix + 10 \\ \hline
ix^2+5x+2 & 2x^3 + 0x^2 + 0x + 0 \\
 & \underline{2x^3 - 10ix^2 - 4ix} \\
 & \quad +10ix^2 + 4ix + 0 \\
 & \quad \underline{+10ix^2 + 50x + 20} \\
 & \qquad (-50+4i)x - 20
\end{array}$$

so that

$$2x^3 = (-2ix + 10)\left(ix^2 + 5x + 2\right) + (-50 + 4i)x - 20,$$

that is

$$q(x) = (-2ix + 10) \text{ and } r(x) = (-50 + 4i)x - 20.$$

Corollary 16.18. *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $(x - a)$.*

Proof. By the division algorithm, there exists $k(x), r(x) \in F[x]$ such that $\deg(r) = 0 < 1$ and

$$f(x) = k(x)(x-a) + r(x). \tag{16.1}$$

Since $\deg(r) = 0$, $r(x) = b$ for some $b \in F$ and hence evaluating Eq. (16.1) at $x = a$ implies,

$$f(a) = k(a)(a-a) + b = b.$$

■

Example 16.19. Let $f(x) = x^2 + 5$ in $\mathbb{R}[x]$. If we divide $(x+1) = (x-(-1))$ into $f(x)$ the remainder will be $f(-1) = 6$.

Example 16.20. If we divide $x - 1$ into $x^2 + 2$ we find,

$$\begin{array}{r} x+1 \\ x-1\overline{)\;x^2 \qquad +2} \\ -x^2+x \qquad \\ \hline x+2 \\ -x+1 \\ \hline 3 \end{array}$$

which gives $x^2 + 2 = (x+1)(x-1) + 3$. Notice that the remainder, $3 = (1)^2 + 2$ as it should be.

Theorem 16.21 ($F[x]$ is a PID). *Let F be a field, then $F[x]$ is a principle ideal domain. Moreover the map,*

$$\{\textit{monic polynomials}\} \ni p \to \langle p\rangle \in \{\textit{non-zero ideals of } F[x]\} \tag{16.2}$$

is a one to one correspondence. The inverse map is given by associating to a non-zero ideal, $I \subset F[x]$, the unique monic polynomial, $p \in I$, with lowest degree.

Proof. Let us first show the map in Eq. (16.2) is one to one. So suppose that p and q are monic polynomials such that $\langle p\rangle = \langle q\rangle$. Then by Lemmas 15.1 and 16.6, we know that $p(x) = kq(x)$ for some $k \in U(F) = F \setminus \{0\}$. Since both p and q are monic, we must in fact have $k = 1$, i.e. $p(x) = q(x)$.

Suppose that $I \subset F[x]$ is an ideal. If $I = \{0\}$ then $I = \langle 0\rangle$ so that $\{0\}$ is a principle ideal (as always). So now suppose that $I \neq \{0\}$ and let $p(x) \in I$ be a non-zero polynomial in I with minimal degree. By dividing $p(x)$ by its leading order coefficient, we may further assume that $p(x)$ is monic. If $f(x) \in I$, use the division algorithm to write, $f(x) = k(x)p(x) + r(x)$ where $\deg(r) < \deg(p)$. Since $r = f - kq \in I$, we must have $r = 0$ showing that $I = \langle p\rangle$ as claimed. If $q \in I$ is another monic polynomial such that $\deg(q) = \deg(p)$, then $q(x) = k(x)p(x)$ for some $k \in F[x]$. A simple degree argument then shows that $\deg(k) = 0$ so that $k(x) = k_0$ is a constant polynomial. Since q and p are both monic, it follows that $k_0 = 1$, i.e. $q(x) = p(x)$. ■

Example 16.22. $\mathbb{Z}[x]$ is not an principle ideal domain. For example consider the ideal,

$$I := \langle 2, x\rangle = \mathbb{Z}[x]\cdot 2 + \mathbb{Z}[x]\cdot x.$$

This ideal is proper since if $1 \in I$, then $1 = 2p(x) + xq(x)$ which would imply that $2p_0 = 1$ for some $p_0 \in \mathbb{Z}$. But this is impossible. If there exists $q \in \mathbb{Z}[x]$ such that $I = \langle q\rangle$, then $2 = q(x)p(x)$ for some p. However this would imply $0 = \deg(2) = \deg(p) + \deg(q)$ from which it follows that $\deg(q) = 0$. Therefore $q(x) = q_0$ for some $q_0 \in \mathbb{Z}$. As I is proper we know that $q_0 \neq \pm 1$ and since $2 \in \langle q_0\rangle$ we must have $q_0 = \pm 2$. However, it should be clear that $x \in I$ while $x \notin \langle 2\rangle = \langle -2\rangle$. Thus I is not a principle ideal.

16.4 Appendix: Proof of the division algorithm

Let us now give the formal proof of Theorem 16.13.

Proof. Proof of Theorem 16.13. Suppose that $f, g \in F[x]$ with $g \neq 0$. We break the proof into the existence and uniqueness assertions.

Uniqueness. Suppose that we have two decompositions,

$$f = qg + r = q'g + r'$$

where $\deg r < \deg g$ and $\deg r' < \deg g$. Then

$$(q - q')g + (r - r') = 0,$$

or equivalently,

$$(q - q')g = (r' - r).$$

If $r - r' \neq 0$, we may take degrees of this equation to conclude,

$$\deg(q - q') + \deg g = \deg(r - r') < \deg g$$

which is a contradiction. Therefore $r = r'$ which then forces $q = q'$ since $F[x]$ is an integral domain and $g \neq 0$.This proves uniqueness.

Existence. Write

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \text{ and}$$
$$g(x) = b_m x^m + \cdots + b_1 x + b_0.$$

If $m = \deg g > \deg f = n$ then we $q = 0$, and $r = f$ so that $f = 0 \cdot g + f$ with $\deg f < \deg g$.

If $m = \deg g \leq \deg f = n$, we will use induction on the degree of f. In the base case, $\deg f = 0$, we have $\deg g = 0$ so that $f = a_0$ and $g = b_0$ and therefore, $f = \frac{a_0}{b_0} g + 0$, so $r = 0$ in this case. Now suppose that $n = \deg f \geq 1$ and the existence has been established for all lower n. Let

$$\begin{aligned}
f'(x) &= f(x) - \frac{a_n}{b_m} x^{n-m} g(x) \\
&= a_n x^n + \cdots + a_1 x + a_0 - \frac{a_n}{b_m} x^{n-m} \left(b_m x^m + \cdots + b_1 x + b_0 \right) \\
&= c_{n-1} x^{n-1} + \cdots + c_0.
\end{aligned}$$

Thus $\deg f' < n$ and hence by the induction hypothesis, $f'(x) = q'(x) g(x) + r(x)$ where $r = 0$ or $\deg(r) < \deg(g)$. Therefore,

$$\begin{aligned}
f(x) &= \frac{a_n}{b_m} x^{n-m} g(x) + f'(x) = \frac{a_n}{b_m} x^{n-m} g(x) + q'(x) g(x) + r(x) \\
&= \left[\frac{a_n}{b_m} x^{n-m} + q'(x) \right] g(x) + r(x) \\
&= q(x) g(x) + r(x)
\end{aligned}$$

where $q(x) = \frac{a_n}{b_m} x^{n-m} + q'(x)$ and $r = 0$ or $\deg(r) < \deg g$. ■

17

Lecture 17

We reviewed Corollary 11.5 in preparation for the next quiz.

17.1 Roots of polynomials

Definition 17.1. *Let R be an integral domain and $f(x) \in R[x]$. Then $a \in R$ is a* ***zero or root*** *of $f(x)$ if $f(a) = 0$.*

Example 17.2. Let $f(x) = 2x^2 + 5x - 7$ in $\mathbb{Z}[x]$. Then $f(1) = 0$ so 1 is a root while $f(2) = 11 \neq 0$ so 2 is not a root of f.

Corollary 17.3. *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $(x - a) \,|\, f(x) \iff f(a) = 0$, i.e. iff a is a root of $f(x)$.*

Remark 17.4. Corollary 17.3 holds more generally in that we may replace F by any commutative ring with identity. Indeed, if $f(x) \in R[x]$ and $f(a) = 0$ for some $a \in R$. Let $g(x) := f(x + a)$, so that $g(x) \in R[x]$ with $g(0) = 0$. Since $g(0) = 0$, $g(x)$ has no constant term which means that we may factor x out of $g(x)$, i.e. $g(x) = xk(x)$ for some $k(x) \in R[x]$. This translates into the statement about $f(x)$;

$$f(x) = g(x - a) = (x - a)\, k(x - a),$$

which shows $x - a$ is a factor of $f(x)$.

Example 17.5. Let $f(x) = x^2 + 5$ has no roots over $\mathbb{R}$ but two roots over $\mathbb{C}$. Indeed,

$$f(x) = \left(x - i\sqrt{5}\right)\left(x + i\sqrt{5}\right)$$

so that $f\left(\pm i\sqrt{5}\right) = 0$.

Example 17.6 (Book Problem 17.13). Consider the polynomial, $f(x) = x^3 + 6$ on $\mathbb{Z}_7[x]$ and observe that

x	0	1	2	3	4	5	6
$f(x)$	6	0	0	5	0	5	5

Thus we know that $(x - 1)$, $(x - 2)$, and $(x - 4)$ are all factors of $f(x)$. For example,

$$\begin{array}{r|l}
 & x^2 + x + 1 \\ \hline
x - 1 & x^3 + 0x^2 + 0x + 6 \\
 & x^3 - x^2 \\ \hline
 & + x^2 + \\
 & + x^2 - x \\ \hline
 & x + 6 \\
 & x - 1 \\ \hline
 & 7 = 0
\end{array}$$

from which it follows that

$$f(x) = (x - 1)\left(x^2 + x + 1\right).$$

Let $g(x) = x^2 + x + 1$ and notice that $0 = f(2) = g(2)$ so that $(x - 2)$ must divide $g(x)$. Indeed this is the case,

$$\begin{array}{r|l}
 & x + 3 \\ \hline
x - 2 & x^2 + x + 1 \\
 & x^2 - 2x \\ \hline
 & + 3x + 1 \\
 & + 3x - 6 \\ \hline
 & 7 = 0
\end{array}$$

from which it follows that

$$g(x) = (x - 2)(x + 3) = (x - 2)(x - 4).$$

Thus as expected, we have

$$f(x) = (x - 1)(x - 2)(x - 4).$$

Corollary 17.7. *Let F be a field, $f(x) \in F[x]$, and suppose that $\{a_i\}_{i=1}^n \subset F$ is a list of n – distinct zeros of f. Then $\prod_{i=1}^n (x - a_i)$ divides $f(x)$. Alternatively put, there exists $k(x) \in F[x]$ such that*

$$f(x) = k(x)(x - a_1)(x - a_2)\ldots(x - a_n). \tag{17.1}$$

Proof. The proof goes by induction on n. When $n = 1$ this is the content of Corollary 17.3. Suppose the result holds for all $k \le n$ for some $n \ge 1$. Then if $\{a_i\}_{i=1}^{n+1}$ is a list of distinct zeros of f, by corollary 17.3, there exists $g(x) \in F[x]$ such that

$$f(x) = g(x)(x - a_{n+1}). \tag{17.2}$$

Since

$$0 = f(a_i) = g(a_i)(a_i - a_n + 1)$$

and $a_i - a_{n+1} \neq 0$ for all $i \le n$, it follows that $\{a_i\}_{i=1}^{n}$ are distinct zeros of g. Therefore by the induction hypothesis, there exists, $k(x) \in F[x]$ such that

$$g(x) = k(x)(x - a_1)(x - a_2)\dots(x - a_n). \tag{17.3}$$

Thus it follows from Eqs. (17.2) and (17.3) that

$$f(x) = k(x)(x - a_1)(x - a_2)\dots(x - a_n)(x - a_{n+1})$$

which completes the induction step and the proof. ∎

Corollary 17.8. *Let F be a field and $f(x) \in F[x]$ with $N := \deg(f)$. Then f has at most N distinct roots in F.*

Proof. If $a_1, \dots, a_n$ be distinct zeros of $f(x)$. Then we may write $f(x)$ as in Eq. (17.1) from which it follows that

$$N = \deg(f) = n + \deg(k) \ge n.$$

∎

Example 17.9. Consider

$$f(x) = (x - 4)(x - 5) = (x + 2)(x + 1) = x^2 + 3x + 2$$

in $\mathbb{Z}_6[x]$. Clearly $f(4) = f(5) = 0$ but this is not all. Indeed, $f(0) = 2 \neq 0$, $f(1) = 3 \cdot 2 = 6 = 0$, $f(2) = 4 \cdot 3 = 12 = 0$, $f(3) = (-1)(-2) = 2 \neq 0$. Thus see that $f(x)$ has four zeros in $\mathbb{Z}_6$, namely $\{1, 2, 4, 5\}$.

Example 17.10 (Zeros of $x^n - 1$). Suppose that $z = re^{i\theta}$ is a zero of $x^n - 1$ in $\mathbb{C}$. Then we must have

$$r^n e^{in\theta} = 1$$

which implies $r = 1$ and $in\theta = k2\pi$ for some $k \in \mathbb{Z}$. Thus the zeros, $\mathcal{Z}$, of $x^n - 1$ are,

$$\mathcal{Z} = \left\{e^{ik2\pi/n} : k \in \mathbb{Z}\right\} = \left\{e^{ik2\pi/n} : k \in \mathbb{Z}_n\right\}.$$

If we let $\omega := e^{i2\pi/n}$, then we may write

$$\mathcal{Z} = \left\{\omega^k : k \in \mathbb{Z}_n\right\}$$

and ω is called a primitive n^{th} – root of unity.

17.2 Roots with multiplicities

Definition 17.11. *Let F be a field and $f(x) \in F[x]$. A root, $a \in F$, of $f(x)$ is said to have **multiplicity** $k \ge 1$ if $(x - a)^k$ divides $f(x)$ but $(x - a)^{k+1}$ does not.*

Example 17.12. In $\mathbb{R}[x]$, 3 is a root of order 2 for $f(x) = x^2 - 6x + 9$. Indeed, $f(x) = (x - 3)^2$. If $f(x) = x^2 - 7x + 10$, then $f(x) = (x - 2)(x - 5)$ and the only zeros of f are $x = 2$ and $x = 5$ each of which have multiplicity 1.

Example 17.13. Since $f(x) = x^3 - 2x^2 + x \in \mathbb{Q}[x]$ factors as,

$$f(x) = x\left(x^2 - 2x + 1\right) = x(x - 1)^2,$$

the roots of $f(x)$ are 0 and 1 with multiplicities 1 and 2 respectively.

Example 17.14. In $\mathbb{R}[x]$ the polynomial, $f(x) = x^4 + 2x^2 + 1$ has no roots. While in $\mathbb{C}[x]$ it has two distinct roots each with multiplicity 2. To find these roots observe that

$$f(x) = \left(x^2 + 1\right)^2 = [(x - i)(x + i)]^2 = (x - i)^2(x + i)^2.$$

Thus the roots are $\pm i$.

Example 17.15 (17.23). Find all of the zeros and multiplicity of

$$f(x) = x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 \in \mathbb{Z}_5[x].$$

We start by finding all of the roots;

x	0	1	2	3	4
$f(x)$	1	0	2	0	3

.

Then we divide $(x - 1)$ into $f(x)$ to find,

$$\begin{array}{r|l}
 & x^4 \; + 4x^2 + 3x - 1 \\ \hline
x - 1 & x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 \\
 & \underline{x^5 - x^4} \\
 & \qquad 4x^3 - x^2 - 4x + 1 \\
 & \qquad \underline{4x^3 - 4x^2} \\
 & \qquad\qquad 3x^2 - 4x + 1 \\
 & \qquad\qquad \underline{3x^2 - 3x} \\
 & \qquad\qquad\qquad - x + 1 \\
 & \qquad\qquad\qquad \underline{- x + 1} \\
 & \qquad\qquad\qquad\qquad 0
\end{array}$$

to find
$$f(x) = (x-1)\, g(x)$$
with $g(x) = x^4 + 4x^2 + 3x - 1$. Let us check we got this right,
$$\begin{aligned}(x-1)\left(x^4+4x^2+3x-1\right) &= x^5 - x^4 + 4x^3 - x^2 - 4x + 1 \\ &= x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1. \checkmark\end{aligned}$$

Notice that $g(1) = 7 \bmod 5 = 2 \neq 0$ so that 1 is a root with multiplicity 1. We now divide $(x-3)$ into $g(x)$ to find;

$$\begin{array}{r}
x^3 \; + 3x^2 + 3x + 2 \\
x-3 \,\big)\, \overline{x^4 + 0x^3 + 4x^2 + 3x - 1} \\
\underline{x^4 - 3x^3} \qquad\qquad\qquad \\
3x^3 + 4x^2 + 3x - 1 \\
\underline{3x^3 - 4x^2} \qquad\qquad \\
+ 3x^2 + 3x - 1 \\
+ \underline{3x^2 - 4x} \quad\;\; \\
+ 2x - 1 \\
+ \underline{2x - 1} \\
0
\end{array}$$

so that
$$g(x) = (x-3)\left(x^3 + 3x^2 + 3x + 2\right).$$
Let $h(x) := x^3 + 3x^2 + 3x + 2$, then $h(3) = 2 \cdot 3^3 + 3^2 + 2 = 65 \bmod 5 = 0$ so that $(x-3)$ goes into $h(x)$. Here is the computation,

$$\begin{array}{r}
x^2 \; + \; x \; + \quad 1 \\
x-3 \,\big)\, \overline{x^3 + 3x^2 + 3x + \quad 2} \\
\underline{x^3 - 3x^2} \qquad\qquad\quad \\
x^2 + 3x + \quad 2 \\
\underline{x^2 \; - 3x} \qquad\quad \\
+ \; x \; + \quad 2 \\
+ \; \underline{x \; - \quad 3} \\
+ 5 = 0
\end{array} .$$

Thus we have shown,
$$x^5 + 4x^4 + 4x^3 - x^2 - 4x + 1 = (x-1)(x-3)^2\left(x^2 + x + 1\right).$$
so that 3 has multiplicity 2. This is rather painful way to carry this out. We will later develop a derivative test to make finding multiplicities easier to determine.

Lecture 18

Corollary 17.7 has the following useful refinement.

Theorem 18.1. *Suppose that $a_1, \ldots, a_n$ are distinct zeros of $f(x) \in F[x]$ with multiplicities, $l_1, \ldots, l_n$. Then there exists $k(x) \in F[x]$ such that*

$$f(x) = k(x)(x - a_1)^{l_1} \ldots (x - a_n)^{l_n}. \tag{18.1}$$

Proof. The proof will be by induction on $N := \sum_{i=1}^n l_i$. If $N = 1$, then we have $n = 1$, $a_1 = a \in F$ and $l_1 = 1$. In this case it follows by definition of a root with multiplicity 1 that $f(x) = k(x)(x - a)$ for some $k(x) \in F[x]$.

Now suppose $N \geq 2$ and the theorem holds whenever $\sum_{i=1}^n l_i < N$. By the induction hypothesis there exists $k_1(x) \in F[x]$ such that

$$f(x) = k_1(x)(x - a_1)^{l_1 - 1}(x - a_2)^{l_2} \ldots (x - a_n)^{l_n}. \tag{18.2}$$

Moreover since $(x - a_1)^{l_1} | f(x)$ it follows that $(x - a_1)$ divides

$$f_1(x) = k_1(x)(x - a_2)^{l_2} \ldots (x - a_n)^{l_n}$$

which implies $f_1(a_1) = 0$. Since $f_1(a_1) = 0$ while

$$(x - a_2)^{l_2} \ldots (x - a_n)^{l_n} |_{x = a_1} \neq 0,$$

we may conclude that $k_1(a_1) = 0$. Therefore that $(x - a_1) | k_1(x)$, i.e. $k_1(x) = k(x)(x - a_1)$ for some $k(x) \in F[x]$. Using this expression for $k_1(x)$ back in Eq. (18.2) completes the proof. ■

Corollary 18.2. *Let F be a field and $f(x) \in F[x]$ with $N := \deg(f)$. Then f has at most N roots in F when counted with multiplicities. In particular, there can be at most N distinct roots of $f(x)$ in F.*

Proof. If $a_1, \ldots, a_n$ be zeros of $f(x)$ with multiplicities, $l_1, \ldots, l_n$. Then from Theorem 18.1 there exists $k(x) \in F[x]$ such that Eq. (18.1) holds. In particular it follows that

$$N := \deg(f) = \deg(k) + \sum_{i=1}^n l_i \geq \sum_{i=1}^n l_i.$$

This inequality is precisely what the Corollary states. ■

18.1 Irreducibles and Maximal Ideals

Definition 18.3. *Let R be an integral domain and $a \in R^\times \backslash U(R)$. We say that a is **reducible** if it admits a **non-trivial factorization**, i.e. $a = bc$ for come $b, c \in R^\times \setminus U(R)$. Otherwise we say that a is **irreducible.** So a is irreducible iff $a \neq 0$, $a \notin U(R)$, and whenever $a = bc$ then either b or c is in $U(R)$.*

Let F be a field and recall from Lemma 16.6 that $U(F[x]) = U(F) = F^\times$. Therefore the associates to $f(x) \in F[x]$ are $\{af(x) : a \in F^\times\}$. So $f(x) = a \cdot h(x)$ with $a \in F^\times$ and $h(x) \in F[x]$ is a trivial factorization.

Example 18.4. If F is a field then $f(x) \in F[x]$ is reducible iff there is a factorization of the form $f(x) = g(x)h(x)$ where $\deg g \geq 1$ and $\deg h \geq 1$.

Lemma 18.5. *If F is a field and $f(x) = g \in F[x]$ is reducible, then* $\deg(f(x)) \geq 2$. *In particular if* $\deg(f(x)) = 1$ *then $f(x)$ is irreducible.*

Proof. If $f(x)$ admits a non-trivial factorization, $f(x) = g(x)h(x)$, then

$$\deg f(x) = \deg h(x) + \deg g(x) \geq 1 + 1 \geq 2.$$

■

Example 18.6. In $\mathbb{Z}[x]$;

1. $x^2 - 1$ is reducible since $x^2 - 1 = (x - 1)(x + 1)$.
2. $2x + 4 = 2(x + 2)$ is reducible in $\mathbb{Z}[x]$ since both 2 and $x + 2$ are not units in $\mathbb{Z}[x]$. Similarly $5x \in \mathbb{Z}[x]$ is reducible since $f(x) = 5 \cdot x$ where both 5 and x are not units.

Notice that $2x + 4 = 2(x + 2)$ is irreducible in $\mathbb{Q}[x]$ by Lemma 18.5. The difference now is that 2 is invertible in $\mathbb{Q}[x]$ while it is not in $\mathbb{Z}[x]$.

Proposition 18.7. *Suppose that D is an integral domain and $0 \neq a \in D \setminus U(D)$. Then a is irreducible iff $\langle a \rangle$ is maximal among all principle ideals in D. To say $\langle a \rangle$ is maximal among all principle ideals in D we mean if $b \in D$ satisfies $\langle a \rangle \subset \langle b \rangle \subset R$, then either $\langle a \rangle = \langle b \rangle$ or $\langle b \rangle = R$.*

Proof. You will prove this in the homework. ■

The following theorem is a direct consequence of Proposition 18.7 and Theorem 14.3.

Theorem 18.8 (p irreducible $\iff$ $\langle p\rangle$ maximal in a PID). *Suppose that D is a PID and $p \in D^{\times} \setminus U(D)$. Then the following are equivalent;*

1. *p is irreducible,*
2. *$\langle p\rangle$ is a maximal ideal, and*
3. *$D/\langle p\rangle$ is a field.*

Example 18.9. In $\mathbb{R}[x]$, x^2+1 is irreducible. Indeed if x^2+1 where to factor non-trivially the factors would have to be linear and x^2+1 would have to have a root which it does not. Consequently we know that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field. We already know this since we have seen, $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to $\mathbb{C}$. Nevertheless, we have now shown that $\mathbb{R}[x]/\langle x^2+1\rangle$ is a field without knowledge about $\mathbb{C}$ and hence we may view this as a fresh construction of $\mathbb{C}$.