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

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

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

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 $M_2(\mathbb{Z})$;

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

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,

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

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 $A = A_1 \cup \cdots \cup A_n$ 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

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

∎

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 $\{a_\lambda\}_{\lambda\in\Lambda}$ and $\{b_\lambda\}_{\lambda\in\Lambda}$ 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

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

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 **principal 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 principal ideal.*

Proof. If $R = \mathbb{Z}$, then $\langle m \rangle = m\mathbb{Z}$ inside of $\mathbb{Z}$ is the principal 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 principal 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

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

where

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

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 $m \geq 2$, 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

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

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

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

while

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

as desired. Secondly,

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

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 $S := \{x^k : k = 0,1,2\ldots\}$ 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 $x = (x_1,\ldots,x_d)$ are d indeterminants and $k = (k_1,\ldots,k_d)$ are multi-indices. Then we let

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

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,

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

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.*

Example 4.2. 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 4.3 ($U(\mathbb{Z}_m) = U(m)$). *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 4.4. 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 4.5. Let R be the non-commuative 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 4.6 (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 4.7 (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 4.8 (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 4.9. 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 4.12 below.

Example 4.10. 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 4.11. *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 4.12. *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 4.13. 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 4.14. 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 4.15. 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 4.16. It is not true that if R is not an integral domain then every sub-ring, $S \subset R$ 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 4.17 (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 4.18. 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 4.19 (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 4.20 (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 4.21. $\mathbb{Z}$ 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 4.22. 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*

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

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

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

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 $\left\{1, \sqrt{2}\right\}$ 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 4.15. 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 $p_1^2|m^2=n^2p_1,\dots,p_k$ 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*

$$\varphi(r_1r_2)=\varphi(r_1)\varphi(r_2)\ \text{and}$$
$$\varphi(r_1+r_2)=\varphi(r_1)+\varphi(r_2)$$

*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 $\varphi=id$.