(i) Let R be a ring with identity. Show that $(R\setminus\{0\}, \times)$ is a group iff $R^* = R\setminus\{0\}$.

SOLUTION: Suppose $R^* = R\setminus\{0\}$. By Theorem 1, $(R^*, \times)$ is a group. Hence $(R\setminus\{0\}, \times)$ is a group. Conversely, suppose $(R\setminus\{0\}, \times)$ is a group. Then all elements in $R\setminus\{0\}$ are invertible, i.e. $R\setminus\{0\} \subseteq R^*$. To show $R\setminus\{0\} = R^*$, it suffices to show that 0 is not invertible. Indeed, if it were, then by LEMMA 5 $R = \{0\}$, whence $R\setminus\{0\} = \emptyset$, which (by convention) is not a group, contradicting the assumption.

(ii) Let H be the set of quaternions, with addition $(+)$ and multiplication $(\times)$ as defined in class. $(H, +)$ is an abelian group. Complete the proof of the fact that $(H, +, \times)$ is a ring.

SOLUTION: We need to verify associativity of the product and left- and right distributivity. Let

$a_0 + a_1 i + a_2 j + a_3 k =: A$

$b_0 + b_1 i + b_2 j + b_3 k =: B$

$c_0 + c_1 i + c_2 j + c_3 k =: C$

be generic quaternions.

It is a routine matter to verify that

$A(B+C) = AB + AC$, $(A+B)C = AB + AC$

and $(AB)C = A(BC)$.

iii a $0 = a0 = a(b+(-b)) = ab + a(-b)$ (using LEMMA 2, defn of $-b$ and distributivity)

$\therefore a(-b) = -ab$

Similarly $(-a)b = -ab$

Now $(-a)(-b) = (-(-a))(-b) = a(-b) = a(-(-b)) = ab$

b $(-1)a = -(-(-1))a = -(1a) = -a$

(using part (a), defn of 1, and that $1+(-1)=0$)

---

iv Let S be a set. Assuming $(\mathcal{P}(S), \Delta)$ is an abelian group, show that $(\mathcal{P}(S), \Delta, \cap)$ is a ring.

SOLUTION:

RTP associativity of Δ and distributivity.

Note, given $x \in S$,

$x \in (A \Delta B) \Delta C \iff \left(\begin{array}{l} x \in A \Delta B \\ \text{and} \\ x \notin C \end{array}\right)$ OR $\left(\begin{array}{l} x \notin A \Delta B \\ \text{and} \\ x \in C \end{array}\right)$

$\iff$

$\left(\begin{array}{l} x \in A \text{ and} \\ x \notin B, x \notin C \end{array}\right)$ OR $\left(\begin{array}{l} x \in B \text{ and} \\ x \notin A, x \notin C \end{array}\right)$ OR $\left(\begin{array}{l} x \in C \text{ and} \\ x \notin A, x \notin B \end{array}\right)$ OR $\left(\begin{array}{l} x \in C \text{ and} \\ x \in A, x \in B \end{array}\right)$

$\iff x$ belongs to precisely 1 or 3 of A, B, C (*)

Now $x \in A \Delta (B \Delta C) \iff x \in (B \Delta C) \Delta A$ (Δ is commutative)

$\iff x$ belongs to precisely 1 or 3 of ABC

where the last equivalence holds by (*) (relabelling $A \leftarrow B$, $B \leftarrow C$, $C \leftarrow A$)

This deals with associativity. As for distributivity,

$x \in A \cap (B \Delta C) \iff x \in A$ and x lies in exactly one of B, C

while

$x \in (A \cap B) \Delta (A \cap C) \iff x$ lies in exactly one of $(A \cap B), (A \cap C)$

$\iff \left(\begin{array}{l} x \in A, x \in B \text{ and} \\ x \notin A \cap C \end{array}\right)$ OR $\left(\begin{array}{l} x \in A, x \in C \text{ and} \\ x \notin A \cap B \end{array}\right)$

$\iff x$ lies in A and in one of B, C. This deals with left-distributivity; right distributivity is similar.

v Given sets S and $A_1, A_2, A_3, \ldots A_n \in \mathcal{P}(S)$, show that $A_1 \Delta A_2 \Delta \cdots \Delta A_n$ consists precisely of the elements $x \in S$ s.t. $|\{i \mid x \in A_i\}|$ is odd.

SOLUTION: By induction on n. For $n=1$ (base case) clearly $x \in A_1$ iff the no. of sets which contain it (chosen from A_1) is one, one being the only odd possibility (the other possibility being zero)

For the inductive step, let $B_n := A_1 \Delta A_2 \cdots \Delta A_n$, and consider $B_{n+1} = B_n \Delta A_{n+1}$. Then

$x \in B_{n+1} \iff x$ is in precisely one of B_n, A_{n+1}

$\iff$ (by inductive hypothesis) (x is in an even no. of sets among $A_1, A_2 \ldots A_n$ and $x \in A_{n+1}$) OR (x is in an odd no. of sets among $A_1, A_2 \ldots A_n$ and $x \notin A_n$)

$\iff x$ is in an odd no. of sets among $A_1, A_2 \ldots, A_{n+1}$

vi Given a set S, consider the ring $(\mathcal{P}(S), \Delta, \cap)$. Establish (with a proof) for which value(s) of $|S|$ (if any) this ring is

a an integral domain (b) a field

SOLUTION: Suppose first $|S| \geq 2$, and pick $a_1, a_2 \in S$, $a_1 \neq a_2$. Recall $\emptyset$ is the zero element in $\mathcal{P}(S)$. Note $\{a_1\} \cap \{a_2\} = \emptyset$ and $\{a_1\} \neq \emptyset \neq \{a_2\}$. Thus $\{a_1\}, \{a_2\}$ are zero-divisors, and $\mathcal{P}(S)$ is not an I.D., and therefore not a field. If $|S| = 0$, i.e., $S = \emptyset$, then $\mathcal{P}(S) = \{\emptyset\}$, the trivial ring, which is neither a field nor an I.D. Finally, if $|S| = 1$, say $S = \{a\}$, from the tables

Δ	$\emptyset$	$\{a\}$
$\emptyset$	$\emptyset$	$\{a\}$
$\{a\}$	$\{a\}$	$\emptyset$

and

$\cap$	$\emptyset$	$\{a\}$
$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$

we see that $\mathcal{P}(S) \cong \mathbb{Z}_2$, which is a field and an I.D.

Thus $\mathcal{P}(S)$ is an I.D., and a field, only if $|S| = 1$.

(vii) Let R be a Boolean ring. Show that

(a) $\forall a \in R,\ a = -a$ (hint: expand $(a+a)^2$)

(b) R is commutative

SOLUTION:

(a) $(a+a) = (a+a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$

$0 = a + a$

$a = -a$

(b) $a+b = (a+b)^2 = a^2 + b^2 + ab + ba = a + b + ab + ba$

$0 = ab + ba = ab - ba$ (by part (a) and Exercise (iii))

$ba = ab$

(viii a) Let S be a subring of a ring R. Show that the zero element of S is the zero element of R

b) Consider the operations $\oplus$, $\otimes$ on $\mathbb{R}^2$ defined by

$(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2,\ y_1 + y_2)$

$(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2,\ y_1 y_2)$

i) Show that $\mathbb{R}^2$, with $\oplus$ for addition and $\otimes$ for multiplication, is a commutative ring with identity, but not an I.D.

ii) Find a subring S with identity, such that the identity of $\mathbb{R}^2$ is distinct from the identity of S.

c) Suppose R is an integral domain, with identity, and S a subring of R, also with identity. Show that, as long as S is non-trivial ($|S| > 1$), the identity of S is the identity of R.

SOLUTION:

a) Let $0_S, 0_R$ denote the zero elements of S, R respectively. Pick $s \in S$.

Then $0_S + s = s = 0_R + s$ (Recall rings are groups w.r.t. $+$, so we may cancel)

$0_S = 0_R$

viii b i Taking $(0,0)$ and $(1,1)$ for the zero and identity elements respectively, all the required axioms — associativity of $\oplus$ and $\otimes$, existence of inverse w.r.t. $\oplus$, neutrality of $(0,0)$, $(1,1)$ w.r.t. $\oplus$, $\otimes$ respectively, commutativity of $\oplus$, $\otimes$, all follow from the corresponding properties of $+$, $\times$ on $\mathbb{R}$. Note however that, for example $(1,0) \otimes (0,1) = (0,0)$, so $(1,0)$, $(0,1)$ are zero-divisors. Hence $\mathbb{R}^2$ is not an I.D.

ii $S := \{(x,0) \mid x \in \mathbb{R}\}$. Clearly S is closed under subtraction of two elements, and multiplication. By the second subring test, S is a subring of R, with identity $(1,0) \neq (1,1)$

(c) Let 1_S, 1_R denote the identity elements of S, R respectively. Pick $s \in S$. Since $|S| > 1$, we may assume $s \neq 0$.

Then $s1_S = s = s1_R$ ⟩ By LEMMA 7 (cancellation law for multiplication, in IDs)

$1_S = 1_R$

(ix) Show that the upper-triangular 2×2 matrices with real entries constitute a ring. (You may assume the set of all 2×2 matrices is a ring. In both cases, $+$ and $\times$ are the usual addition and multiplication of matrices.)

SOLUTION Let $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$, $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ be arbitrary upper-triangular 2×2 matrices. Then

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix}, \text{ and}$$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}.$$

Since both resulting matrices are upper triangular, the set of upper triangular matrices is closed under multiplication and subtraction of two elements; by the 2nd subring test, it is a subring and in particular a ring.

x) Show that, if $R[x]$ has the identity element, then R also must have the identity element and that the identity element of $R[x]$ is the constant polynomial corresponding to the identity element of R

SOLUTION:

Let e be the identity element of $R[x]$, $e = \sum_{i=0}^{n} a_i x^i$

Then $\forall p \in R[x] \quad ep = p$.

In particular, $\forall k \in R$, seen as the constant polynomial

$$ek = k, \quad \text{i.e.}$$

$$(a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n)\, k = k$$

Therefore, considering the constant term on either side,

$$a_0 k = k \qquad \text{Note this holds } \forall K \in R$$

Hence a_0 is the identity element of R. But then a_0 is also the identity element of $R[x]$ (as a constant polynomial), because if $\sum_{i=0}^{s} b_i x^i$ is an arbitrary element of $R[x]$,

$$a_0 (b_0 + b_1 x + b_2 x^2 + \dots + b_s x^s) =$$

$$a_0 b_0 + a_0 b_1 x + \dots + a_0 b_s x^s =$$

$$b_0 + b_1 x + \dots + b_s x^s$$

—

xi) Show that, if φ is a ring isomorphism, so is φ^{-1}.

SOLUTION: Note that the inverse of a bijection is always a bijection: φ^{-1} is 1-1 simply because φ is well-defined, i.e. $\varphi(x)$ is uniquely determined by x, and φ^{-1} is onto simply because φ is defined on all of its domain.

RTP φ^{-1} is a homomorphism. Let R, S be the domain and codomain of φ (respectively), so that

$$\varphi : R \to S \qquad \varphi^{-1} : S \to R.$$

Pick $a, b \in S$. Then $\exists x, y \in R$ s.t. $a = \varphi(x)$, $b = \varphi(y)$ (since φ is onto)

(xi) (cont.) Note $a+b = \varphi(x)+\varphi(y) = \varphi(x+y)$ (since φ is a homomorphism)
and $ab = \varphi(x)\varphi(y) = \varphi(xy)$

But then $\varphi^{-1}(a+b) = x+y = \varphi^{-1}(a)+\varphi^{-1}(b)$
and $\varphi^{-1}(ab) = xy = \varphi^{-1}(a)\varphi^{-1}(b)$, as required.

(xii) Given a ring R, consider the condition

$$\forall a_1, b_1, a_2, b_2 \in R \quad \left.\begin{matrix} a_1 \sim b_1 \\ a_2 \sim b_2 \end{matrix}\right\} \Rightarrow \begin{cases} a_1 + a_2 \sim b_1 + b_2 \\ a_1 a_2 \sim b_1 b_2 \end{cases} \quad (*)$$

Let $\sim$ be an equivalence relation on R such that $(*)$ holds, let C be any equivalence class, and put $I(C) := \{x-y \mid x, y \in C\}$. Show that:

(a) $\Delta \in I(C) \Rightarrow \forall a \in R,\ a \sim a+\Delta$

(b) $I(C)$ does not depend on the equivalence class C

(c) $I(C)$ is a subgroup of R (w.r.t. $+$).

SOLUTION:

(a) Given $\Delta \in I(C)$, $\Delta = x_2 - x_1$ for some $x_1, x_2 \in C$
Then of course $(a-x_1)+x_1 = a$. But $x_1 \sim x_2$ (since they belong to same class)
Hence by $(*)$ $(a-x_1)+x_2 \sim a$ (note $a-x_1 \sim a-x_1$)
that is, $a+(x_2-x_1) \sim a$
or $a+\Delta \sim a$

(b) Let C_1, C_2 be arbitrary equivalence classes. To see $I(C_1) \subseteq I(C_2)$, pick $\Delta \in I(C_1)$, and also $a \in C_2$. By part (a), $a \sim a+\Delta$, i.e. a, $a+\Delta$ belong to the same equivalence class. But $a \in C_2$, so $a+\Delta \in C_2$. Hence $\Delta = (a+\Delta)-a \in I(C_2)$. We conclude that $I(C_1) \subseteq I(C_2)$ and the argument applies with C_2 and C_1 in each other's rôle, so that $I(C_2) \subseteq I(C_1)$ and $I(C_1) = I(C_2)$.

(c) Pick $x \in C$. Then $x \sim x$ so $0 = x-x \in I(C)$. Thus $I(C) \neq \emptyset$.
To see $I(C)$ is closed under taking inverses (negatives), pick $\Delta \in I(C)$. Then $\Delta = x-y$ for some $x, y \in C$.

By definition of $I(c)$, $-\Delta = y - x \in I(c)$.
Hence $I(c)$ is closed under taking negatives.
To see $I(c)$ is closed under addition, pick $\Delta_1, \Delta_2 \in I(c)$, and $a \in C$.
Then $a \sim a + \Delta_1 \sim (a + \Delta_1) + \Delta_2 = a + (\Delta_1 + \Delta_2)$ (by part (a))
$\therefore \quad a + (\Delta_1 + \Delta_2) - a \in I(c)$ (by defn of $I(c)$)
i.e. $\Delta_1 + \Delta_2 \in I(c)$
We conclude $I(c)$ is non-empty and closed under addition as well as taking negatives, and is therefore a subgroup.

xiii Let I be a subgroup of a ring R. Consider the binary relation on R defined by

$$x \sim y \iff x - y \in I$$

Show that $\sim$ is an equivalence relation.

SOLUTION:

Since I is a subgroup, it contains 0. Therefore, $\forall x \in R$, $x - x \in I$, whence $x \sim x$. Thus $\sim$ is reflexive.

Since I is a subgroup, it is closed under taking negatives. Hence, $\forall x, y \in R$

$$x \sim y \Rightarrow x - y \in I \Rightarrow y - x \in I \Rightarrow y \sim x$$

Thus $\sim$ is symmetric.

Since I is a subgroup, I is closed under subtraction. Hence, $\forall x, y, z \in R$

$$x \sim y \sim z \Rightarrow x - y \in I,\ y - z \in I \Rightarrow (x - y) - (y - z) \in I$$
$$\Rightarrow x - z \in I$$
$$\Rightarrow x \sim z$$

Thus $\sim$ is transitive, as well as reflexive and symmetric. We conclude $\sim$ is an equivalence relation.

xiv (a) Recall, $\forall n \in \mathbb{N}$, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Consider the factor ring $\mathbb{Z}/n\mathbb{Z}$, and the equivalence relation defined by

$$x \sim y \iff x - y \in n\mathbb{Z}$$

(a) Show that, given $a \in \mathbb{Z}$, if we find $q, r \in \mathbb{Z}$ such that

$$a = qn + r \quad \text{with} \quad 0 \leq r < n,$$

then $a \sim r$

(b) Deduce that $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.

SOLUTION:

(a) $a = qn + r \Rightarrow a - r = qn \Rightarrow a - r \in n\mathbb{Z} \Rightarrow a \sim r$

(b) Recall the definition of $\mathbb{Z}_n$ (Tuesday 5th February) and that of a factor ring (THM 5, Thursday March 13th). According to $\sim$, two integers are equivalent iff they differ by a multiple of n. Thus the elements of $\mathbb{Z}/n\mathbb{Z}$ are precisely the elements of $\mathbb{Z}_n$ (equivalence classes of integers modulo n). To see the operations on $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ coincide, recall that, to add (multiply) two classes C_1, C_2 in $\mathbb{Z}/n\mathbb{Z}$, we may pick any representative of each, add (multiply) in $\mathbb{Z}$, and then take the class containing the result. But this is exactly what we do in $\mathbb{Z}_n$, representing the resulting class by the remainder upon division by n.

(xv) Show that, given any ideal I in a ring R, if

(a) R is commutative; or

(b) R has the identity element

then the same holds for R/I. Give an example of an integral domain with a factor ring that is not an integral domain.

(xv) (cont.) SOLUTION:

(a) Given $C_1, C_2 \in R/I$, pick $x_1 \in C_1$, $x_2 \in C_2$. Then

$$C_1 \times C_2 = [x_1 x_2] = [x_2 x_1] = C_2 \times C_1$$

(b) We claim $[1]$ is the identity element of R/I. In fact, given $C \in R/I$, pick $a \in C$. Then

$$C[1] = [a1] = [a] = C$$

For the required example, it is sufficient to take $\mathbb{Z}_4$ as a factor ring of $\mathbb{Z}$, the latter being an integral domain, while the former is not, since

$$\bar{2} \times \bar{2} = \bar{0} \qquad (\text{or } [2] \times [2] = [0])$$

implying that $\bar{2}$ is a zero-divisor.

(xvi) Given a subset S of a commutative ring R, show that S coincides with the set of finite linear combinations of distinct elements of S.

SOLUTION: Let U denote the set of finite linear combinations of distinct elements of S. Clearly $U \subseteq \langle S \rangle$. To see $\langle S \rangle \subseteq U$, consider an arbitrary finite linear combination of (not necessarily distinct) elements of S, i.e.

$$\sum_{i=0}^{n} a_i s_i \qquad \text{where, } \forall i = 1, \ldots, n, \; a_i \in R, \; s_i \in R$$

Now if K is the set $\{s_i\}_{i=1,\ldots,n}$, using distributivity we may write

$$\sum_{i=0}^{n} a_i s_i = \sum_{s \in K} \left(\sum_{i : s_i = s} a_i \right) s$$

which is a finite linear combination of distinct elements of S.

xvii Given a ring R, and a collection $\{I_j\}_{j\in J}$ of ideals of R, show that $\bigcap_{j\in J} I_j$ is an ideal of R (as long as it is non-empty). Show moreover that if R is a commutative ring with identity, and $\emptyset \subseteq S \subseteq R$, then $\langle S\rangle$ is the smallest ideal in R containing S.

SOLUTION:

We apply the ideal test to $I := \bigcap_{j\in J} I_j$. To check that I is closed under subtraction, pick $x, y \in I$. Then, $\forall j \in J$, $x, y \in I_j$, and since I_j, being an ideal, is closed under subtraction, $\forall j \in J$ $x - y \in I_j$. Therefore $x - y \in I$.

To check that I absorbs products, pick $z \in I$, $r \in R$. Then $\forall j \in J$, $z \in I_j$, and since I_j, being an ideal, absorbs products, $\forall j \in J$ $rz \in I_j$ and $zr \in I_j$. Therefore $rz \in I$ and $zr \in I$.

By the ideal test, I is an ideal (assuming it is non-empty)

Now suppose R is commutative, and has the identity element. Note $\langle S\rangle$ is an ideal (LEMMA 12). Moreover, $S \subseteq \langle S\rangle$ because any $a \in S$ can be written as the trivial linear combination $1a$. It remains to be shown that, if I is any ideal containing S, then $\langle S\rangle \subseteq I$. Indeed, given any finite linear combination of elements of S, these elements also belong to I, which absorbs products and therefore also contains the multiples, and is closed under addition and therefore contains the entire linear combination.

xviii) Give an example of a ring homomorphism $\varphi: R \to S$ and an ideal $I \subseteq R$ such that $\varphi(I)$ is not an ideal of S.

SOLUTION: It is sufficient to take $R := \mathbb{Z}$, $S := \mathbb{R}$, $I := \mathbb{Z}$, and $\varphi : \mathbb{Z} \to \mathbb{R}$

$$x \mapsto x$$

Clearly φ is a homomorphism, but $\varphi(\mathbb{Z}) = \mathbb{Z}$ is not an ideal, since it does not absorb all products, e.g. $\frac{1}{2}(1) = \frac{1}{2} \notin \mathbb{Z}$.

xix)

(a) Given integers a, b, show that, in the ring $\mathbb{Z}$,

$$\langle a \rangle \subseteq \langle b \rangle \iff b \mid a$$

(b) Assuming $\mathbb{Z}$ is a principal ideal domain, deduce that, $\forall n \geq 0$ $\langle n \rangle$ is maximal $\iff$ n is a prime integer

SOLUTION:

(a) Suppose $b \mid a$. Then $\exists k \in \mathbb{Z}$ s.t. $bk = a$. Hence every multiple of a is also a multiple of b. But $\langle b \rangle, \langle a \rangle$ consist precisely of the multiples of b, a respectively (using Exercise xvi). So $\langle a \rangle \subseteq \langle b \rangle$.

Conversely, suppose $\langle a \rangle \subseteq \langle b \rangle$. Since $a = a1 \in \langle a \rangle$, $a \in \langle b \rangle$, i.e. $\exists k \in \mathbb{Z}$ s.t. $a = bk$, whence $b \mid a$.

(b) First we observe that $\langle n \rangle = \mathbb{Z} \iff n = 1$, and $\langle 0 \rangle = \{0\}$. Since $0, 1$ are not prime integers, and $\{0\}, \mathbb{Z}$ are not maximal ideals of $\mathbb{Z}$, the assertion is true for $n = 0, 1$. So w.m.a. $n \geq 2$. Suppose $\langle n \rangle$ is not maximal. Then there exists an ideal I of $\mathbb{Z}$ s.t.

$\langle n \rangle \subsetneq I \subsetneq \mathbb{Z}$. Since $\mathbb{Z}$ is a P.I.D., $I = \langle k \rangle$ for some $k \in \mathbb{Z}$. Since $\langle k \rangle = \langle -k \rangle$, we may assume $k \geq 0$. Now $\langle n \rangle \subsetneq \langle k \rangle \subsetneq \mathbb{Z}$. By part (a), $k \mid n$.

(xix)(b) (cont) Since $\langle k \rangle \neq \mathbb{Z}$, $k \neq 1$, and since $\langle k \rangle \neq \langle n \rangle$, $k \neq n$. Thus $1 \neq k \neq n$, $k > 0$ and $n = kp$ for some $p \in \mathbb{Z}$, implying n is not prime.

Conversely, suppose n is not prime. Then $n = pq$ for some p, q s.t. $1 < p, q < n$

Again by part (a), $\langle n \rangle \subseteq \langle p \rangle$. Since $n = n1 \in \langle n \rangle$, to show $\langle n \rangle$ is not maximal, it is sufficient to show $p \notin \langle n \rangle$, implying $\langle n \rangle \subsetneq \langle p \rangle$. (note also $\langle p \rangle \subsetneq \mathbb{Z}$). Indeed, $p \in \langle n \rangle$ would imply $p = kn$ for some (positive) k, whence $p \geq n$, whereas we have $p < n$, a contradiction.

(xx) Given an integral domain R and a subring $S \subseteq R$ consisting of at least two elements, show that S is an integral domain

SOLUTION:

S contains at least two elements by assumption, and is commutative, being a subring of R, which is an integral domain and therefore commutative. Moreover, S does not have any zero-divisors, as these would also be zero-divisors in the integral domain R (note, by Exercise (xviii, a), the zero elements in R and S coincide).

Thus S is an integral domain.

xxi a Let R be a Euclidean ring. Given a non-zero element $p \in R$, show that any non-zero element of $R/\langle p \rangle$ (coset of $\langle p \rangle$ in R) has a representative $r \neq 0$ such that $N(r) < N(p)$ (where N is a norm on R).

SOLUTION: Let the coset C be a non-zero element of $R/\langle p \rangle$. Note $\langle p \rangle$ is the zero element of $R/\langle p \rangle$. Pick $a \in C$.

By the division property of Euclidean rings, there exist $q, r \in R$ s.t. $a = qp + r$ where $r = 0$ or $N(r) < N(p)$ (and $r \neq 0$)

First we show that $r = 0$ is impossible. Indeed

$r = 0 \Rightarrow a = qp \Rightarrow a \in \langle p \rangle$.

But C, $\langle p \rangle$ are distinct, therefore disjoint, cosets.

At the same time $a \in C$. Thus $r = 0$ gives a contradiction.

Hence $r \neq 0$ and $N(r) < N(p)$. Now it suffices to show $r \in C$. But recall, $\forall x, y \in R$

x, y are equivalent $\Leftrightarrow x - y \in \langle p \rangle$

Taking $x = a$, $y = r$, $x - y = a - r = qp \in \langle p \rangle$

so a, r are equivalent, i.e. $r \in C$, as required.

---

b Suppose now $R = D[x]$, where D is an integral domain. Given distinct $s, t \in R \setminus \{0\}$, show that, if $\deg(s) < \deg(p) > \deg(t)$, then s, t belong to distinct cosets.

SOLUTION: Suppose, by way of contradiction, that s, t belong to the same coset. Then $s - t \in \langle p \rangle$, that is,

$\exists z \in D[x]$ s.t. $s - t = zp$.

Since $s \neq t$, $s - t \neq 0$. Hence $z \neq 0$. Since D is an integral domain, $\deg(s - t) = \deg(z) + \deg(p) \geq \deg(p)$.

But $\deg(s - t) = \deg(s + (-t))$

$\leq \max\{\deg(s), \deg(-t)\}$

$= \max\{\deg(s), \deg(t)\} < \deg(p)$, a contradiction.

Note on xi b) It is important in the above that R is of the form $D[x]$.
Suppose $R = \mathbb{G}$, the Gaussian integers, and take $p = 5$, $s = 3$, $t = -2$. Note $N(s) = 9 < 25 = N(p)$ and

$$N(t) = 4 < 25 = N(p)$$

Yet s, t belong to the same coset because $s - t = 5 \in \langle 5 \rangle$

---

xi c) Suppose further that $D = \mathbb{Z}_7$ and $p = x^{10} + 1$. How many elements does $R/\langle p \rangle = \mathbb{Z}_7[x]/\langle x^{10}+1 \rangle$ have? Find a formula in terms of $|D|$ and $\deg(p)$ to generalize this to the case when D is a finite field and p is any non-zero polynomial.

SOLUTION: Consider the set S of polynomials of the form $\sum_{i=0}^{9} a_i x^i$, where $a_i \in \mathbb{Z}_7$ $(\forall i = 0, \ldots, 9)$, and the mapping $\gamma : S \to \mathbb{Z}_7[x]/\langle p \rangle$. We claim γ is a bijection.

$s \mapsto [s]$

To see injectivity, pick $s, t \in S$, $s \neq t$.
If s, t are both non-zero, then by (b) $[s] \neq [t]$.
So suppose $s = 0$, $t \neq 0$, and, by way of contradiction, that $[s] = [t]$, i.e. $[t] = [0]$.

Then $t - 0 = t \in \langle x^{10}+1 \rangle$, i.e. $\exists z \in D[x]$ s.t. $t = z(x^{10}+1)$
Since $t \neq 0$, $z \neq 0$ and since D is an integral domain
$\deg(t) = \deg(x^{10}+1) + \deg(z) \geq 10$. But
$\deg(t) \leq 9$, a contradiction.

Similar to previous argument in (b).

As for surjectivity, pick $C \in R/\langle x^{10}+1 \rangle$.
If C is non-zero, by part (a)
$\exists r \in S$ s.t. $C = [r] = \gamma(r)$.
If C is the zero element of $R/\langle x^{10}+1 \rangle$, then $C = [0]$
Thus γ is a bijection, and the required number is $|S|$.

Now any element of S is obtained by choosing each of the 10 coefficients from the 7 elements of $\mathbb{Z}_7$. Thus $|S| = 7^{10}$.

This generalizes to $\left|D[x]/\langle p\rangle\right| = |D|^{\deg(p)}$ $(p \neq 0)$.

(xxii) Show that $\mathbb{C}$ and $\mathbb{R}[x]/\langle x^2+1\rangle$ are isomorphic. Deduce that $\langle x^2+1\rangle$ is a maximal ideal.

SOLUTION: Since $\mathbb{R}$ is a field, $\mathbb{R}[x]$ is a Euclidean ring and Exercise (xxi) applies. So we may represent the cosets in $\mathbb{R}[x]/\langle x^2+1\rangle$ by polynomials of degree $< \deg(x^2+1) = 2$, i.e. polynomials of the form $a+bx$ where $a, b \in \mathbb{R}$ are arbitrary, and the mapping

$$\varphi : \mathbb{C} \longrightarrow \mathbb{R}[x]/\langle x^2+1\rangle$$
$$a+bi \longmapsto [a+bx]$$

is a bijection. We claim it is a homomorphism. In fact, given arbitrary complex numbers $a+bi$, $c+di$

$$\varphi((a+bi)+(c+di)) = \varphi((a+c)+(b+d)i) = [(a+c)+(b+d)x]$$
$$= [a+bx] + [c+dx]$$
$$= \varphi(a+bi) + \varphi(c+di)$$

and

$$\varphi((a+bi)(c+di)) = \varphi((ac-bd)+(ad+bc)i)$$
$$= [(ac-bd)+(ad+bc)x]$$

while

$$\varphi(a+bi)\varphi(c+di) = [a+bx][c+dx]$$
$$= [ac+(ad+bc)x+bdx^2]$$

But in the factor ring, we may change representatives of a coset by adding/subtracting a multiple of (x^2+1), so

$$[ac+(ad+bc)x+bdx^2] = [ac+(ad+bc)x+bdx^2-bd(x^2+1)]$$
$$= [(ac-bd)+(ad+bc)x]; \text{ as required.}$$

Hence $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$. We know $\mathbb{C}$ is a field; by Proposition 2 (Tuesday 8th April), the ideal $\langle x^2+1\rangle$ is maximal.

xxiii Let R be a Euclidean ring, with norm N. Show that

(a) the minimum value of $N(x)$, for $x \in R \setminus \{0\}$, occurs when $x = 1$

(b) $\forall u \in R \setminus \{0\}$, $N(u) = N(1) \iff u \in R^*$

Deduce that $G^* = \{1, -1, i, -i\}$, where G denotes the ring of Gaussian integers

SOLUTION:

(a) $\forall x \in R \setminus \{0\}$, $N(x) = N(1x) \geq N(1)$

(b) Spse $u \in R^*$. By (a), we have $N(u) \geq N(1)$.

Moreover, $N(u) \leq N(uu^{-1}) = N(1)$. Hence $N(u) = N(1)$

Conversely, spse $N(u) = N(1)$. By the division property of Euclidean rings, there exist q, r such that $1 = qu + r$

(i) $r = 0$ or (ii) $r \neq 0$ and $N(r) < N(u)$

But $N(u) = N(1)$ so, by part (a), (ii) is impossible

Hence $r = 0$ and $1 = qu$. Thus $u \in R^*$.

In order to find G^*, note that $1 = 1 + 0i$ is the identity element of G, and $N(1) = 1^2 + 0^2 = 1$. Thus by (b) $a + bi \in G$ is a unit iff $a^2 + b^2 = 1$

Now note that, $\forall a, b \in \mathbb{Z}$, $(a \neq 0) \wedge (b \neq 0) \Rightarrow a^2 + b^2 \geq 1 + 1 = 2$. Thus $a^2 + b^2 = 1$ requires that one of a, b be 0, and consequently the other one should be ± 1. This leaves four possibilities: $a = 0$, $b = \pm 1$, and $b = 0$, $a = \pm 1$.

Clearly all four satisfy $a^2 + b^2 = 1$.

Hence $G^* = \{1, -1, i, -i\}$

xxiv) Let R be a commutative ring with identity. Show that the binary relation $\approx$ on R defined by

$x \approx y \Leftrightarrow x$ is an associate of y

is an equivalence relation.

SOLUTION:

$x \approx y \Rightarrow x = uy$ for some $u \in R^*$

$\Rightarrow y = u^{-1}x$

$\Rightarrow y \approx x$ (note $u^{-1} \in R^*$)

Thus $\approx$ is symmetric. Moreover, $\forall x \in R$, $x = 1x$, therefore $x \approx x$. Thus $\approx$ is reflexive.

Furthermore

$x \approx y \approx z \Rightarrow x = u_1 y$, $y = u_2 z$ for some $u_1, u_2 \in R^*$

$\Rightarrow x = u_1 u_2 z$

$\Rightarrow x \approx z$ (note $u_1, u_2 \in R^*$)

Thus $\approx$ is transitive as well as symmetric and reflexive. We conclude $\approx$ is an equivalence relation.

(xxv) Given a positive integer n, consider the set of complex numbers $\mathbb{G}_n := \{a + b\sqrt{n}\, i \mid a, b \in \mathbb{Z}\}$.

(a) Show that $\mathbb{G}_n$ is a ring and an integral domain.

(b) For $z \in \mathbb{G}_n$, put $N(z) := |z|^2$ ($\mathbb{G}_n$ may or may not be a Euclidean ring) Show that

$x | y$ in $\mathbb{G}_n \Rightarrow N(x) \mid N(y)$ in $\mathbb{Z}$

(c) Now suppose $n = 5$, and put $a := 6$, $b = 2(1 + \sqrt{5}\, i)$. Show that, in $\mathbb{G}_5$, a and b do not have a gcd (Hint: Note $6 = (1 + \sqrt{5}\, i)(1 - \sqrt{5}\, i) = 3 \cdot 2$)

SOLUTION:

(a) To show $\mathbb{G}_n$ is a ring, it is sufficient to show it is a subring of $\mathbb{C}$. Pick $x, y \in \mathbb{G}_n$. Then $x = a + b\sqrt{n}\, i$ $y = c + d\sqrt{n}\, i$ for some $a, b, c, d \in \mathbb{Z}$. Then $x - y = (a - c) + (b - d)\sqrt{n}\, i$ and $xy = (a + b\sqrt{n}\, i)(c + d\sqrt{n}\, i) = (ac - bdn) + (ad + bc)\sqrt{n}\, i$

Since a, b, c, d, n are all integers, so are $a - c$, $b - d$, $ac - bdn$, $ad + bc$. Thus $x - y$, $xy \in \mathbb{G}_n$, and $\mathbb{G}_n$ is closed under subtraction and products. By the second subring test, $\mathbb{G}_n$ is a subring of $\mathbb{C}$.

To see that $\mathbb{G}_n$ is an integral domain, note that any zero-divisors in $\mathbb{G}_n$ would also be zero-divisors in $\mathbb{C}$. But $\mathbb{C}$ is a field so no such zero-divisors exist. Moreover, commutativity holds in $\mathbb{C}$, and therefore (in particular) in $\mathbb{G}_n$. Finally, clearly $\mathbb{G}_n \neq \{0\}$. Thus $\mathbb{G}_n$ is indeed an integral domain.

b) If $x|y$ in $\mathbb{G}_n$, then $\exists k \in \mathbb{G}_n$ s.t. $y = kx$. Then

$|y| = |kx| = |k||x|$ (multiplicativity of the absolute value is known to hold in $\mathbb{C}$, ∴ in $\mathbb{G}_n$, but can also easily be shown directly)

Therefore

$|y|^2 = |k|^2 |x|^2$, i.e.

$N(y) = N(k)N(x)$. Hence

$N(x) \mid N(y)$ (recall N takes values in $\mathbb{Z}$).

c) Suppose, by way of contradiction, that a, b have a gcd x, and put $X := N(x)$. Since $6 = (1+\sqrt{5}i)(1-\sqrt{5}i) =$

$(1+\sqrt{5}i) \mid 6$. Thus $1+\sqrt{5}i$ is a common divisor of $a = 6$ and $b = 2(1+\sqrt{5}i)$. The same is true of 2.

Since x is a gcd, $2|x$ and $(1+\sqrt{5}i) \mid x$ (in $\mathbb{G}_5$)

By (b) $N(2) \mid N(x)$ and $N(1+\sqrt{5}i) \mid N(x)$ (in $\mathbb{Z}$)

i.e. $4 \mid X$ and $6 \mid X$

$\therefore 12 \mid X$

But $x|a \Rightarrow N(x) \mid N(a)$ i.e. $X \mid 36$

and $x|b \Rightarrow N(x) \mid N(b)$ i.e. $X \mid 24$

$\Rightarrow X = 12$

But if $x = a+bi$ $(a, b \in \mathbb{Z})$

$X = a^2 + b^2$

So $a^2 + b^2 = 12$

Note $0^2 = 0$ $1^2 = 1$ $2^2 = 4$ $3^2 = 9$ and $a \geq 4 \Rightarrow a^2 \geq 16$

Thus 12 is a sum of two of $0, 1, 4, 9$, which is clearly impossible.

xxvi | Let R be an integral domain with identity. Show that $(R[x])^* = R^*$

SOLUTION.

Note first that the constant polynomial 1 is the identity element of $R[x]$.

Suppose first $u \in R^*$.

Then there exists $k \in R$ such that

$$uk = 1$$

This equation holds in R, but also in $R[x]$ when $u, k, 1$ are viewed as constant polynomials. Thus $u \in (R[x])^*$.

Since u was chosen arbitrarily in R^*, we have that $R^* \subseteq (R[x])^*$.

Conversely, suppose $p \in (R[x])^*$

Then there exists $q \in R[x]$ such that

$$p(x)\,q(x) = 1$$

Since R is an integral domain (and therefore has at least two elements), $1 \neq 0$.

Hence p, q are both non-zero, and we have

$$\deg(p) + \deg(q) = \deg(1) = 0$$

But $\deg(p), \deg(q) \geq 0$, so we must have

$$\deg(p) = \deg(q) = 0,$$

i.e. p, q are (non-zero) constant polynomials.

Thus the equation

$$pq = 1$$

holds in R as well as $R[x]$, and in particular $p \in R^*$. Since p was chosen arbitrarily in $(R[x])^*$, we have that $(R[x])^* \subseteq R^*$ and therefore $(R[x])^* = R^*$.

(xvii) (a) Spse $u \in G_5^*$. Then $uz = 1$ for some $z \in \mathbb{Z}$. Therefore, by Exercise (xxvb), $N(u) \mid N(1)$. But $N(1) = 1$ and $N(u) \geq 0$. Since the only factors of 1 are ± 1, we conclude $N(u) = 1$. Now if $u = a + b\sqrt{5}\,i$, we have $N(u) = a^2 + 5b^2 = 1$. Thus the only possibilities are $u = \pm 1$, both of which are indeed invertible ($1 \times 1 = 1$, $(-1)(-1) = 1$).

(b) Since $G_5^* = \{1, -1\}$, clearly neither of $3, 2$ is an associate of $1 + \sqrt{5}\,i$ or $1 - \sqrt{5}\,i$. To see G_5 is not a UFD, it remains to be shown that $1 \pm \sqrt{5}\,i$, 2 and 3 are irreducible. For suppose

$$(a + b\sqrt{5}\,i)(c + d\sqrt{5}\,i) = 1 \pm \sqrt{5}\,i \,/\, 2 \,/\, 3$$

Then $(a^2 + 5b^2)(c^2 + 5d^2) = 6/4/9$

But any factorization of $6/4/9$ into positive integers and avoiding 1 must involve 2 or 3, neither of which can be written in the form $x^2 + 5y^2$ $(x, y \in \mathbb{Z})$.

Hence $a^2 + 5b^2 = 1$ or $c^2 + 5d^2 = 1$,

so one of the factors $a + bi$, $c + di$ is ± 1, i.e. the factorization is trivial. We conclude $1 \pm \sqrt{5}\,i$, 2, 3 are all irreducible.

(xxviii) Let R be an integral domain with identity element. Given $a \in R$, $a \neq 0$, suppose $a = bc$ is a non-trivial factorization ($b, c \notin R^*$). Show that $\langle a \rangle \subsetneq \langle b \rangle$.

SOLUTION: Clearly every multiple of a is also a multiple of b, so $\langle a \rangle \subseteq \langle b \rangle$. Since $b = b1 \in \langle b \rangle$, it is now sufficient to show $b \notin \langle a \rangle$. Suppose, by way of contradiction, that $b \in \langle a \rangle$. Then $b = ak$ for some $k \in R$, and $a1 = a = bc = akc$, whence $1 = kc$, implying $c \in R^*$, a contradiction.

(xxix) Find all the gcd's of

•) $a = x^3+2x^2+2$ and $b = x^2+2x+1$, in $\mathbb{Z}_3[x]$

••) $a = 18-i$, and $b = -7+8i$, in the ring of Gaussian integers

•••) $a = 2695$, and $b = 493$, in the ring of integers.

In each case, express one of the gcds as a linear combination of a and b (giving the coefficients explicitly).

ANSWERS:

• gcds are $x+1$, $2x+2$

$x+1 = (x)(x^3+2x^2+2) + (2x^2+1)(x^2+2x+1)$

•• gcd's are $1, -1, i, -i$

$1 = (-5i)(18-i) + (6-6i)(-7+8i)$

••• gcd's are $1, -1$

$1 = (-15)(2695) + (82)(493)$