EXERCISES 1

Please submit solutions by 3pm on Thursday 15th February to the pigeonholes in 4W (ground floor)

(W) = Warm-up; (H) = Homework; (A)=Additional.

1. (W) *This exercise illustrates why cosets were introduced at the end of Algebra 1A, at least in the special case where the group G is abelian.* Let $(G, +)$ be an abelian group and let H be a subgroup of G. Define a relation on G by setting $a \sim b \iff a - b \in H$ for $a, b \in G$. Show that:

(1) $\sim$ is an equivalence relation, where the equivalence classes are precisely the subsets in G of the form $a + H = \{a + h \in G \mid h \in H\}$ for $a \in G$ (these sets are the *cosets* of H in G);

(2) the sum of two cosets given by $(a+H)+(b+H) = (a+b)+H$ is well-defined [Hint: for $a, b, a', b' \in G$ satisfying $a \sim a'$ and $b \sim b'$, show that $a + b \sim a' + b'$], and hence show that the set of cosets of H in G is an abelian group.

The set of cosets with the operation from (2) is an abelian group G/H called the *quotient* of G by H.

2. (W) Let R be a ring with 1. Show that if 0 is a unit, then the only element in R is 0.

3. (W) Let R be a ring. Show that the set $M_n(R)$ of all $n \times n$ matrices over R is a ring with respect to the usual matrix addition and multiplication of matrices. If R is a ring with 1, is $M_n(R)$ a ring with 1?

4. (H) Let R be a ring, and let $R[[x]]$ denote the ring of formal power series with coefficients in R. Show that if R is an integral domain, then so is $R[[x]]$.

5. (H) Let $(R, +, \cdot)$ be a ring. Show that a nonempty subset S of R is a subring if and only if $(S, +, \cdot)$ is a ring. [Hint: Lemma 1.5 does some of the work for you.] Deduce that the set of *Gaussian integers*

$$\mathbb{Z}[i] := \left\{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}, i^2 = -1\right\}$$

becomes a ring in which the operations are the usual addition and multiplication of complex numbers.

6. (A) Let S be a given set and let $R = \mathcal{P}(S)$ denote the power set of S, that is, the set containing all subsets of S. For each $A \in R$ let $\overline{A} = S \setminus A$. We define two binary operations on R as follows:

$$A + B = (A \cap \overline{B}) \cup (B \cap \overline{A}) \quad \text{and} \quad A \cdot B = A \cap B.$$

Show that $(R, +, \cdot)$ is a Boolean ring in which the zero element is the emptyset and S is the multiplicative identity. [Hint: It can be useful here to apply the De Morgan laws $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ and $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.]

The course website is: `http://people.bath.ac.uk/ac886/teaching/algebra2B/`

---

1. (1) Let $a, b, c \in G$. Then $a - a = 0 \in H$ means $a \sim a$, so $\sim$ is reflexive. If $a \sim b$ then $a - b \in H$ and hence $b - a = -(a-b) \in H$ by Lemma 1.5. This gives $b \sim a$, so $\sim$ is symmetric. Finally if $a \sim b$ and $b \sim c$ then $a-b, b-c \in H$. As H is closed under addition, it follows that $(a-b)+(b-c) = a-c \in H$ and hence $a \sim c$. This shows that $\sim$ is transitive, so $\sim$ is an equivalence relation.

To compute the equivalence classes, note that the equivalence class of $a \in G$ is

$$\begin{aligned} [a] &:= \{b \in G \mid b \sim a\} \\ &= \{b \in G \mid b - a \in H\} \\ &= \{b \in G \mid \exists\, h \in H \text{ such that } b - a = h\} \\ &= \{a + h \mid h \in H\} \\ &= a + H \end{aligned}$$

as claimed.

(2) Let $a, b, a', b' \in G$ and suppose that $a \sim a'$ and $b \sim b'$. Then $a - a', b - b' \in H$. Since H is a subgroup, we have

$$(a + b) - (a' + b') = (a - a') + (b - b') \in H,$$

so $a + b \sim a' + b'$ as required.

We use this to check that addition is well-defined for cosets. For this, consider alternative representatives of the cosets $a+H$ and $b+H$, say $a' \in G$ satisfying $a+H = a'+H$ and $b' \in G$ satisfying $b + H = b' + H$. Then $a \sim a'$ and $b \sim b'$ and hence $a + b \sim a' + b'$ by above, so

$$\begin{aligned} a' + H + b' + H &= (a' + b') + H && \text{by definition} \\ &= (a + b) + H && \text{as } a + b \sim a' + b' \\ &= a + H + b + H && \text{by definition,} \end{aligned}$$

as required. This shows that addition is a binary operation on the set of cosets G/H. To check that $(G/H, +)$ is an abelian group, we switch to equivalence class notation $[a] = a + H$ (to save space). Note that for $a, b, c \in G$ we have

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]),$$

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

Also, we have $[a]+[0] = [a+0] = [a]$, so $[0]$ is the zero element. Moreover, $[a]+[-a] = [a+(-a)] = [0]$, so $[-a]$ is the additive identity of $[a]$.

2. If 0 is a unit, then there exists $0^{-1} \in R$. Lemma 1.8(a) implies that $1 = 0 \cdot 0^{-1} = 0$. Therefore, for any $a \in R$, we have $a = a \cdot 1 = a \cdot 0 = 0$, i.e., R is the zero ring $\{0\}$.

Note in passing that if $0 = 1$, then R is the zero ring; to rule this out, we often assume $0 \neq 1$.

3. The fact that $(M_n(R), +)$ is associative and commutative follows from the fact that $(R, +)$ is an abelian group. The matrix $0_{n\times n}$ in which every entry is 0 is clearly the additive identity. If $A = (a_{ij}) \in M_n(R)$ then the matrix $B = (b_{ij})$ satisfying $b_{ij} = -a_{ij}$ is an additive inverse of A. Thus $(M_n(R), +)$ is an abelian group.

To see that multiplication is associative, let $A = (a_{ij}), B = (b_{ij})$ and $C = (c_{ij})$ be matrices in $M_n(R)$. Let $D = (d_{ij})$ and $E = (e_{ij})$ where $D = AB$ and $E = BC$. The (i, j)th entry of $(AB)C = DC$ is then

$$\sum_{k=1}^{n} d_{ik}c_{kj} = \sum_{k=1}^{n}\left(\sum_{l=1}^{n} a_{il}b_{lk}\right)c_{kj} = \sum_{l=1}^{n} a_{il}\left(\sum_{k=1}^{n} b_{lk}c_{kj}\right) = \sum_{l=1}^{n} a_{il}e_{lj}$$

which is the (i, j)th entry of $AE = A(BC)$; we applied here both the assocative law for the ring multiplication of R and the distributive law for R. This gives $(AB)C = A(BC)$ as required.

For the distributive laws, the (i, j)th entry of $A(B + C)$ is

$$\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} = u_{ij} + v_{ij}$$

where u_{ij}, v_{ij} are the (i, j)th entries of AB and AC respectively; here we use the distributive law for R as well as the fact that addition is commutative. Hence $A(B + C) = AB + AC$. Similarly one sees that $(B + C)A = BA + CA$.

If R is a ring with 1, then let $\mathbb{I}_n := (\delta_{i,j})$ be the matrix with 1 on the diagonal and 0 elsewhere. Then for any $A \in M_n(R)$, we have $A \cdot \mathbb{I}_n = A = \mathbb{I}_n \cdot A$, so $\mathbb{I}_n$ makes $M_n(R)$ into a ring with 1.

4. By inspecting the formula for multiplication of formal power series

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\right) x^k.$$

we see that the power series $1 = 1+0x+0x^2+0x^3+\cdots$ provides a multiplicative identity for $R[[x]]$, making $R[[x]]$ a ring with 1. Also, looking at the same multiplication formula, notice that if R is commutative then $a_i b_j = b_j a_i$, and hence

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) = \sum_{k=0}^{\infty}\left(\sum_{i+j=k} a_i b_j\right) x^k = \left(\sum_{k=0}^{\infty} b_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} a_k x^k\right)$$

so $R[[x]]$ is commutative. Also, since $0 \neq 1$ in R, the same holds in $R[[x]]$. Finally, if $\sum_{k=0}^{\infty} a_k x^k$ and $\sum_{k=0}^{\infty} b_k x^k$ are two nonzero elements in $R[[x]]$, then $m \in \mathbb{N}$ be the smallest index for which $a_m \neq 0$ and let $n \in \mathbb{N}$ be the smallest index for which $b_n \neq 0$. Then we claim that

$$\left(\sum_{k=0}^{\infty} a_k x^k\right) \cdot \left(\sum_{k=0}^{\infty} b_k x^k\right) = a_m b_n x^{m+n} + (a_{m+1}b_n + a_m b_{n+1})x^{m+n+1} + \dots \tag{0.1}$$

is nonzero. Indeed, since R is an integral domain and since $a_m \neq 0$ and $b_n \neq 0$, we have that $a_m b_n \neq 0$, so the coefficient of x^{m+n} in the expression (0.1) is nonzero. This proves the claim, and completes the proof that $R[[x]]$ is an integral domain.

5. Let S be a subring of R. Since S is nonempty and since the condition from the definition of subring holds, the additive version of Lemma 1.5 shows that $(S, +)$ is a group. This group is abelian, because addition commutes in R. The second condition from the definition of subring implies that multiplication is a binary operation on S. In the ring $(R, +, \cdot)$, we have that $\cdot$ is associative and that the distributive laws hold, so the same is true in $(S, +, \cdot)$. This shows that $(S, +, \cdot)$ is a ring.

Conversely, if $(S, +, \cdot)$ is a ring then S is nonempty (as it contains 0), and it's closed under both subtraction and multiplication, so S is a subring.

We have $0+i0\in\mathbb{Z}[i]$, so $\mathbb{Z}[i]$ is nonempty. For any $a+ib, c+ib\in\mathbb{Z}[i]$ we have

$$(a+ib)-(c+id)=(a-c)+i(b-d)\in\mathbb{Z}[i] \quad\text{ and }\quad (a+ib)(c+id)=(ac-bd)+i(ad+bc)\in\mathbb{Z}[i]$$

since $a,b,c,d\in\mathbb{Z}$ implies that $a-c, b-d, ac-bd, ad+bc\in\mathbb{Z}$. Therefore $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$, so it's a ring in its own right.

6. We first need to check that all the axioms for rings are fullfilled. Addition commutes because

$$A+B=(A\cap\overline{B})\cup(B\cap\overline{A})=(B\cap\overline{A})\cup(A\cap\overline{B})=B+A,$$

and $\emptyset$ is the zero element because

$$A+\emptyset=\emptyset+A=(A\cap\overline{\emptyset})\cup(\emptyset\cap\overline{A})=(A\cap S)\cup\emptyset=A.$$

As for the additive inverse, we've been asked to show that R is a Boolean ring, so the additive inverse of A must equal A itself, so we check this:

$$A+A=(A\cap\overline{A})\cup(A\cap\overline{A})=\emptyset.$$

As is often the case, the hardest part in checking the group axioms is associativity. Here, notice that

$$\begin{aligned}
(A+B)+C &= ((A+B)\cap\overline{C})\cup(\overline{A+B}\cap C)\\
&= ((A\cap\overline{B})\cup(\overline{A}\cap B))\cap\overline{C})\cup((\overline{A\cap\overline{B})\cup(\overline{A}\cap B}))\cap C)\\
&= ((A\cap\overline{B})\cup(\overline{A}\cap B))\cap\overline{C})\cup((\overline{A\cap\overline{B}})\cap(\overline{\overline{A}\cap B})\cap C)\\
&= ((A\cap\overline{B})\cup(\overline{A}\cap B))\cap\overline{C}\cup((\overline{A}\cup B)\cap(A\cup\overline{B})\cap C)\\
&= (A\cap\overline{B}\cap\overline{C})\cup(\overline{A}\cap B\cap\overline{C})\cup(\overline{A}\cap\overline{B}\cap C)\cup(A\cap B\cap C).
\end{aligned}$$

This last expression is completely symmetric in A,B,C, so it's equal to $(B+C)+A=A+(B+C)$.

To check the mulitplicative properties, notice that intersection of sets is an associative operation, so $\cdot$ is associative. Also, we have $A\cap S=S\cap A=A$, so S is the multiplicative identity. It remains to check that R satisfies the distributive laws. We have

$$\begin{aligned}
C\cdot A+C\cdot B &= C\cap A\cap\overline{C\cap B}\cup C\cap B\cap\overline{C\cap A}\\
&= C\cap A\cap(\overline{C}\cup\overline{B})\cup C\cap B\cap(\overline{C}\cup\overline{A})\\
&= C\cap A\cap\overline{C}\cup C\cap A\cap\overline{B}\cup C\cap B\cap\overline{C}\cup C\cap B\cap\overline{A}.
\end{aligned}$$

Now no element can be both in C and in $\overline{C}$ and thus the last expression is equal to.

$$C\cap A\cap\overline{B}\cup C\cap B\cap\overline{A}=C\cap(A\cap\overline{B}\cup B\cap\overline{A})=C\cdot(A+B).$$

Hence $C\cdot(A+B)=C\cdot A+C\cdot B$. Intersection of sets is a commutative operation, so we also have

$$(A+B)\cdot C=C\cdot(A+B)=C\cdot A+C\cdot B=A\cdot C+B\cdot C$$

as required. This shows that R is a ring, and it's Boolean because $A\cdot A=A\cap A=A$.