GROUPS AND RINGS. PROBLEM SHEET 4 SOLUTIONS

ALEXEI N. SKOROBOGATOV

1. Which of the following are rings? Which are integral domains?

(1) The set of rationals a/b with $a, b \in \mathbb{Z}$ and b odd (usual $+$, $\times$).
(2) The set of rationals a/b with $a, b \in \mathbb{Z}$ and b a power of 2 (usual $+$, $\times$).
(3) $\mathbb{Z}$, with new addition $\oplus$ and multiplication $\otimes$ defined by

$$m \oplus n = m + n + 2 \text{ and } m \otimes n = mn + 2m + 2n + 2.$$

Solution:

A subset S of a ring R is a subring $\Leftrightarrow$ $1 \in S$ and for all $a, b \in S$ we have $a + b$, ab and $-a \in S$.

(1) and (2) One easily checks the ring axioms. Note that these are subrings of $\mathbb{Q}$ and therefore integral domains.

(3) Again, it is easy to verify the ring axioms: the additive identity is -2 and the multiplicative identity is -1. If $m \otimes n = -2$ then $mn + 2m + 2n + 4 = 0$, so $(m + 2)(n + 2) = 0$ and $m = -2$ or $n = -2$. Thus, there are no zero divisors.
Note that this ring is isomorphic to $\mathbb{Z}$ with the usual addition and multiplication via the map which sends n to $n - 2$.

2. Let R be a ring. Deduce directly from the axioms of a ring that for any $x, y \in R$ we have $(-x)(-y) = xy$.

Solution:

We have $0 = x \cdot 0 = x(y + (-y)) = xy + x(-y)$. Similarly, $0 = (x + (-x))(-y) = x(-y) + (-x)(-y)$. The desired identity follows.

3. Let $F = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

(1) Prove that F is a field.
(2) Prove that $\mathbb{Q}$ has exactly one subfield (namely $\mathbb{Q}$ itself).
(3) Prove that F has exactly two subfields.

Solution:

(1) Assume that $r = a + b\sqrt{2} \neq 0$. Then $a^2 - 2b^2 \neq 0$: indeed, if $a^2 - 2b^2 = 0$, then $b \neq 0$ (since $r \neq 0$) and hence $(\frac{a}{b})^2 = 2$, which is impossible since a and b are rational numbers. Therefore $\frac{a - b\sqrt{2}}{a^2 - 2b^2}$ belongs to F and is the inverse of r. The rest is easy.

(2) Suppose that $K \subseteq \mathbb{Q}$ with K a field. Then $1 \in K$ and hence $a \in K$ for all $a \in \mathbb{Z}$. Hence $b^{-1} \in K$ for all non-zero $b \in \mathbb{Z}$. Thus, $a/b \in K$ and $K = \mathbb{Q}$.

(3) Let K be a subfield of F. Then $\mathbb{Q} \subseteq K$, as in part (2). Assume that $K \neq \mathbb{Q}$. Then $r = a + b\sqrt{2} \in K$ for some $a, b \in \mathbb{Q}$ with $b \neq 0$. Then $\sqrt{2} = (r - a)b^{-1} \in K$ (since $a, b \in K$). Hence $K = F$.

4. Prove that $\mathbb{Q}$ contains infinitely many subrings which are integral domains.

Date: November 30, 2021.

Solution: Use the example of Question 1 (2) with 2 replaced by any prime p.

5. (Quaternions) Let $\mathbb{H}$ be the set of 2×2 matrices which is given by

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} : z, w \in \mathbb{C} \right\}.$$

Prove that $\mathbb{H}$ is a division ring.

Solution:

$\mathbb{H}$ is a subset of the vector space $\mathbb{C}^2$ and is closed under addition and multiplication by real numbers, so it is a vector space over $\mathbb{R}$, and has a basis consisting of

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The ring axioms hold for $\mathbb{H}$ because they hold for the ring of (2×2)-matrices, and it is easy to check that $\mathbb{H}$ is closed under multiplication. A direct verification gives

$$(x\mathbf{1} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k})(x\mathbf{1} - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}) = x^2 + y^2 + z^2 + w^2.$$

Thus the multiplicative inverse of $x\mathbf{1} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k} \neq 0$ is

$$\frac{x\mathbf{1} - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}}{x^2 + y^2 + z^2 + w^2}.$$

Hence $\mathbb{H}$ is a division ring.

6. Prove that if F_1 and F_2 are subfields of a field K then $F_1 \cap F_2$ is a subfield of K.

Solution: $F_1 \cap F_2$ is closed under the four field operations. The field axioms hold in $F_1 \cap F_2$ because they hold in F_1.

7. Let I and J be ideals of a commutative ring R. Define

$$I + J = \{a + b : a \in I \text{ and } b \in J\}.$$

Prove that $I + J$ is an ideal of R.

Solution: The set $I + J$ is a subgroup of the additive group of R, and is closed under multiplication by the elements of R.

8. Suppose that F is a finite field with p^n elements. Prove that $r^{p^n} = r$ for all $r \in F$.

Solution: The multiplicative group $F^\times$ has $p^n - 1$ elements. By Lagrange's theorem, we have $r^{p^n - 1} = 1$. This implies that $r^{p^n} = r$, which also holds for $r = 0$, so holds for every $r \in F$.

9. Let R be a ring in which $x^2 = x$ for all $x \in R$. Prove that R is commutative.

Solution: For any $x, y \in R$ we have $x + y = (x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2 = (x + y) + (xy + yx)$, hence $xy = -yx$. But $-1 = (-1)^2 = 1$, thus $xy = yx$.