Show all your work. Justify your solutions. Answers without justification will not receive full marks.

Only hand in the problems on page 2.

Practice Problems

Question 1. Prove that an intersection of normal subgroups of G is a normal subgroup of G.

Solution: Let G be a group, H_i a family of normal subgroups with i varying across an index set I, and let $H = \bigcap_{i\in I} H_i$. From class we know that H is a subgroup of G.

Let $g \in G$ and $h \in H$. We must show that $g^{-1}hg \in H$. Since $h \in H$, $h \in H_i$ for each i, so $g^{-1}hg \in H_i$ since $H_i \trianglelefteq G$. So $g^{-1}hg \in \bigcap_{i\in I} H_i = H$.

Question 2. Define operations $\oplus$ and $\odot$ on $\mathbb{Q}$ by $a \oplus b = a + b + 1$, $a \odot b = ab + a + b$. Is $(\mathbb{Q}, \oplus, \odot)$ an integral domain? Is it a field? What happens if $\mathbb{Q}$ is replaced with $\mathbb{Z}$?

Solution: We first show that $(\mathbb{Q}, \oplus, \odot)$ is an integral domain.

$\boxed{\oplus \text{ is associative}}$ For all $a, b, c \in \mathbb{Q}$ we have $(a\oplus b)\oplus c = (a+b+1)\oplus c = a+b+1+c+1 = a+b+c+2$ and $a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$ so $\oplus$ is associative.

$\boxed{\oplus \text{ is commutative}}$ $a \oplus b = a + b + 1 = b + a + 1 = b \oplus a$.

$\boxed{\text{Additive identity}}$ $a \oplus (-1) = a + (-1) + 1 = a = (-1) \oplus a$ so -1 is the additive identity. Denote it by $\mathbb{0}$.

$\boxed{\text{Additive inverses}}$ If $a \oplus b = \mathbb{0} = -1$ then $a + b + 1 = -1$ so $b = -2 - a$. That is, $a \oplus (-2 - a) = a + (-2 - a) + 1 = -1$ so a has additive inverse $(-2 - a)$, which we can denote $\ominus a$.

Thus $(\mathbb{Q}, \oplus)$ is an abelian group.

$\boxed{\odot \text{ is associative}}$ $(a\odot b)\odot c = (ab+a+b)\odot c = (ab+a+b)c+(ab+a+b)+c = abc+ab+bc+ca+a+b+c$, and $a \odot (b \odot c) = a \odot (b + c + bc) = a(b + c + bc) + a + (b + c + bc) = abc + ab + bc + ca + a + b + c$, so $\odot$ is associative.

$\boxed{\odot \text{ is commutative}}$ $a \odot b = ab + a + b = ba + b + a = b \odot a$.

$\boxed{\text{Distributive laws}}$ $a\odot(b\oplus c) = a\odot(b+c+1) = a(b+c+1)+a+(b+c+1) = ab+ac+2a+b+c+1$ and $(a\odot b)\oplus(a\odot c) = (ab+a+b)\oplus(ac+a+c) = (ab+a+b)+(ac+a+c)+1 = ab+ac+2a+b+c+1$. The other distributive law follows because $\odot$ is commutative: $(x \oplus y) \odot z = z \odot (x \oplus y) = (z \odot x) \oplus (z \odot y)$ by above $= (x \odot z) \oplus (y \odot z)$.

$\boxed{\text{Multiplicative identity}}$ If $a \odot e = a$ then $ae + a + e = a$ so $0 = ae + e = (a + 1)e$ for all a, so the only possibility is $e = 0$. And indeed $a \odot 0 = a \cdot 0 + a + 0 = 0 + a + 0 = a$, so $a \odot 0 = a = 0 \odot a$ for all a, so 0 is the multiplicative identity. Denote it by $\mathbb{1}$.

$\boxed{\text{Zero divisors}}$ If $a \odot b = \mathbb{0}$ is the zero element then $a + b + ab = -1$ so $(a + 1)(b + 1) = 0$. So $a = -1 = \mathbb{0}$ or $b = -1 = \mathbb{0}$. Hence there are no zero-divisors.

We have proved that $(\mathbb{Q}, \oplus, \odot)$ is an integral domain.

$\boxed{\text{Units}}$ Suppose $a \neq \mathbb{0}$. We try to find a multiplicative inverse for a, ie solve $a \odot b = \mathbb{1}$ (the multiplicative identity). If this holds then $a + b + ab = 0$ so $b(a + 1) = -a$ so $b = -a/(a + 1)$, which

is valid, since $a \neq -1$ (ie $a \neq \mathbb{0}$). So every non-zero $a \in \mathbb{Q}$ has a multiplicative inverse in $\mathbb{Q}$. Thus $(\mathbb{Q}, \oplus, \odot)$ is a field.

$\boxed{\mathbb{Z}}$ Clearly $\mathbb{Z}$ is closed under $\oplus$ and $\odot$, and contains $\mathbb{0}$ and $\mathbb{1}$. Also if $a \in \mathbb{Z}$ then its additive inverse $\ominus a = -2 - a \in \mathbb{Z}$. Thus $(\mathbb{Z}, \oplus, \odot)$ is a subring of $(\mathbb{Q}, \oplus, \odot)$, and a subring of an integral domain is automatically an integral domain so $(\mathbb{Z}, \oplus, \odot)$ is an integral domain. However it is not a field since $a^{-1} = -a/(a+1) \notin \mathbb{Z}$ in general.

Assignment Problems

Question 1.

(a) Let A be the set of real matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, and let B be the set of real matrices of the form $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, where a and b are non-zero reals. Prove that $G = A \cup B$ is a group under matrix multiplication.

(b) Prove that A is a subgroup of G, and find the cosets of A in G.

(c) Show that $A \trianglelefteq G$.

(d) Show that the set of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is a normal subgroup of A.

(e) Deduce that "a normal subgroup of a normal subgroup" is not necessarily normal (so normality is not transitive).

Solution: (a) Clearly G is non-empty and contains the identity. Since a, $b \neq 0$, if $X \in G$ then $\det X \neq 0$ so X is invertible, and by the formula for the inverse of 2×2 matrices, its inverse is in G. Now let X, $Y \in G$. We show $XY \in G$.

Case $X \in A$, $Y \in A$: a product of diagonal matrices is diagonal, so $XY \in A$.

Case X, $Y \in B$. Say $X = \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$. Then $XY = \begin{pmatrix} ad & 0 \\ 0 & bc \end{pmatrix} \in G$.

Case X and Y in opposite subsets of G. Say $X = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $Y = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$. Then $XY = \begin{pmatrix} 0 & ac \\ bd & 0 \end{pmatrix} \in G$ and $YX = \begin{pmatrix} 0 & bc \\ ad & 0 \end{pmatrix} \in G$, so this accounts for all possibilities.

(b) If $X = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $Y = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ then $XY^{-1} = \begin{pmatrix} a/c & 0 \\ 0 & b/d \end{pmatrix} \in A$, so A is a subgroup of G.

(c) Let $X = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $Y \in G$. We must show $Y^{-1}XY \in A$. This is clear if $Y \in A$, so let $Y = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$. Then $Y^{-1}XY = \begin{pmatrix} 0 & 1/d \\ 1/c & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} = \begin{pmatrix} bd/c & 0 \\ 0 & ac/d \end{pmatrix} \in A$.

(d) Let K be the set of matrices described. If $X = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $Y = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} \in K$ then $XY^{-1} = \begin{pmatrix} a/b & 0 \\ 0 & 1 \end{pmatrix} \in K$, so K is a subgroup of A. Let $Z = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} \in A$. Then $Z^{-1} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} Z = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in K$, so $K \trianglelefteq A$.

Slicker proof: define $f \colon A \to \mathbb{R}$ by $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mapsto d$. Check that this is a homomorphism with kernel K. Kernels are always normal subgroups. Note also that A is abelian, so its subgroups are automatically normal.

(e) Claim: $K \not\trianglelefteq G$. Proof: Let $X = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in A$ and $Y = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \in G$. Then $Y^{-1}XY = \begin{pmatrix} d/c & 0 \\ 0 & ac/d \end{pmatrix}$ by (c). So if $ac \neq d$ then $Y^{-1}XY \notin K$.

Question 2. Let M be the set all 2×2 real matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Show that $M \simeq \mathbb{C}$ as rings.

Solution: Define a map $\mathbb{C} \to M$ by $f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. This is surjective by definition of M and if $f(a+bi) = f(c+di)$ equating the top rows of the matrices shows $a+bi = c+di$, so f is a bijection.

$$\begin{aligned} f\Big((a+bi)+(c+di)\Big) &= f\Big((a+c)+(b+d)i\Big) = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = f(a+bi) + f(c+di) \end{aligned}$$

and

$$\begin{aligned} f(a+bi)f(c+di) &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} \\ &= f\Big((ac-bd)+(ad+bc)i\Big) = f\Big((a+bi)(c+di)\Big). \end{aligned}$$

So f is a homomorphism.

Neat facts: the trace of $f(z)$ is $2 \operatorname{Im} z$ and the determinant is $|z|^2$.

Question 3. Let $\mathscr{F} = \{f \mid f\colon \mathbb{R} \to \mathbb{R}\}$. Composition of functions $(f,g) \mapsto f \circ g$ is a binary operation on $\mathscr{F}$. Is $(\mathscr{F}, +, \circ)$ a ring?

Solution: **No** (but so close!)

From class we know that $(\mathscr{F}, +)$ is an abelian group, and composition of functions is associative, so $(\mathscr{F}, \circ)$ is a semigroup. The remaining properties to check are the two distributive laws.

Let f, g, $h \in \mathscr{F}$. We prove that $(f+g) \circ h = f \circ h + g \circ h$. Let and $x \in \mathbb{R}$. Then

$$\begin{aligned} \Big((f+g)\circ h\Big)(x) &= (f+g)\Big(h(x)\Big) && \text{Def of } \circ \\ &= f\Big(h(x)\Big) \;+\; f\Big(g(x)\Big) && \text{Def } f+g \\ &= (f\circ h)(x) + (f\circ g)(x) && \text{Def } \circ \\ &= \Big(f\circ h \;+\; f\circ g\Big)(x) && \text{Def } + \end{aligned}$$

Thus $\Big((f+g)\circ h\Big)(x) = \Big(f\circ h \;+\; f\circ g\Big)(x)$ for all $x \in \mathbb{R}$, so $(f+g)\circ h = f\circ h \;+\; f\circ g$.

However the other distributive law $f \circ (g+h) = f \circ g + f \circ h$ fails. If we try the same proof:

$$\begin{aligned} \Big(f \circ (g+h)\Big)(x) &= (f\Big((g+h)(x)\Big) && \text{Def of } \circ \\ &= f\Big(g(x)+h(x)\Big) && \text{Def } g+h \end{aligned}$$

But we now write $f\Big(g(x)+h(x)\Big) = f(g(x)) + f(h(x))$. This is essentially the statement $f(a+b) = f(a)+f(b)$, which certainly does not hold for all real functions. To get a counter-example, we should choose f to be non-linear.

Thus, let $f(x) = x^2$, $g(x) = x$, $h(x) = x$. Then $\Big(f \circ (g+h))(x) = f\Big((g+h)(x)\Big) = f(g(x)+h(x)) = f(2x) = 4x^2$. But $(f \circ g + f \circ h)(x) = (f \circ g)(x) + (f \circ h)(x) = f(g(x)) + f(h(x)) = f(x) + f(x) = x^2 + x^2 = 2x^2$, so $\Big(f \circ (g+h)\Big)(x) \neq \Big(f \circ g + f \circ h\Big)(x)$ for some values of x (such as $x = 1$). Hence $f \circ (g+h) \neq (f \circ g \ + \ f \circ h)$.

Thus $(\mathscr{F}, +, \circ)$ satisfies all the axioms to be a ring, except the distributive law $f \circ (g+h) = f \circ g + f \circ h$. [This shows that both distributive laws really are needed in the definition of a ring; one cannot be derived from the other.]

To get a ring, we would have to take the subset of $f \in \mathscr{F}$ satisfying $f(a+b) = f(a) + f(b)$.