**MATH3195/M5195 EXERCISE SHEET 1**
**SOLUTIONS**

DUE: FEBRUARY 5, 2020

Warm-up exercises

**Problem 1.** Work out the example from the first lecture: What are the integer solutions of $x^2 + y^2 = z^2$?
(1) First show that the rational solutions of $X^2 + Y^2 = 1$ are of the form

$$(X, Y) = \left(\frac{-2m}{1+m^2}, \frac{1-m^2}{1+m^2}\right), m \in \mathbb{Q}, \quad \text{and } (X, Y) = (0, -1)\,.$$

(2) From this find the integer solutions of the original equation.

**Solution.** (1) Think of the solution set as a circle in $\mathbb{R}^2$. Consider a line of slope $m$ through $(0, 1)$ that rotates about $(0, 1)$. This will give us all rational points on the circle except $(0, -1)$ (which would correspond to the slope $m = \infty$). So we can then find all solutions of our new equation by using $m$ as a new parameter. So we want rational solutions of

$$\left.\begin{array}{c} y - mx = 1 \\ X^2 + Y^2 = 1 \end{array}\right\}$$

Substituting the first of these into the second we see

$$\begin{aligned} X^2 + (mX + 1)^2 = 1 &\implies X^2 + m^2X^2 + 2mX + 1 = 1 \\ &\implies X^2(m^2 + 1) + 2mX = 0 \\ &\implies X\left(X(m^2 + 1) + 2m\right) = 0. \end{aligned}$$

This gives two solutions, $X = 0$ and $X = \dfrac{-2m}{m^2+1}$. The first solution for $X$ gives $Y = 1$, and the second gives

$$Y = \frac{-2m^2}{m^2+1} + 1 = \frac{1-m^2}{1+m^2}.$$

Note that $m = 0$ also yields the solution $(0, 1)$. The solutions are therefore

$$(X, Y) = (0, -1) \text{ and } (X, Y) = \left(\frac{-2m}{1+m^2}, \frac{1-m^2}{1+m^2}\right) \ (m \in \mathbb{R}).$$

We need to see which values of $m$ give rational values of $X$ and $Y$. A bit of checking shows that $X, Y \in \mathbb{Q} \iff m \in \mathbb{Q}$. So let $m = \frac{p}{q}$, where $p$ and $q$ are coprime integers. Then

$$X = \frac{-2pq}{p^2+q^2} \text{ and } Y = \frac{q^2-p^2}{p^2+q^2}.$$

(2) Returning to our original variables $x$, $y$ and $z$ we see that integer solutions to $x^2 + y^2 = z^2$ can be given by

$$x = -2pq,\ y = q^2 - p^2,\ z = p^2 + q^2, \quad p, q \in \mathbb{Z},\ p, q \text{ coprime, or}$$

$$x = -pq,\ y = \frac{q^2 - p^2}{2},\ z = \frac{p^2 + q^2}{2} \quad \text{if both } p \text{ and } q \text{ are odd.}$$

For instance, $p = 1, q = 3$ gives $x = 3, y = 4, z = 5$.

**Problem 2.** Let $\mathbb{T} = (\mathbb{R} \cup \{\infty\}, \oplus, \odot)$ with addition defined as $x \oplus y := \min(x, y)$ and multiplication $x \odot y := x + y$ for all $x, y \in \mathbb{R} \cup \{\infty\}$.

(a) Is $\mathbb{T}$ a commutative ring? If yes, then show that all axioms hold, if no, then explain which axiom fails.
(b) Calculate $3 \odot (5 \oplus 7)$, $(3 \oplus -3)^2$, and $(1 \oplus 8)^4$.
(c) Show that for any $x, y \in \mathbb{R} \cup \{\infty\}$, and any $k \in \mathbb{N}$, one has $(x \oplus y)^k = x^k \oplus y^k$.

**Solution.** For (a) note that $\min(x, \infty) = x$ for any $x \in \mathbb{T}$, which means that $0_{\mathbb{T}} = \infty$. The multiplicative unit is the "normal" additive unit, that is $1_{\mathbb{T}} = 0$. The multiplication $\odot$ is associative and commutative since the addition in $\mathbb{R} \cup \{\infty\}$ is associative and commutative. For the addition $\oplus$ write out:

$$a \oplus (b \oplus c) = a \oplus \min(b, c) = \min(a, \min(b, c)) = \min(a, b, c) = \min(\min(a, b), c) = (a \oplus b) \oplus c\ .$$

Commutativity is clear, because $\min(a, b) = \min(b, a)$. Thus $\oplus$ is associative, commutative and the neutral element is $\infty$. Distributivity comes from

$$a \odot (b \oplus c) = a + \min(b, c) = \min(a + b, a + c) = (a + b) \oplus (a + c) = (a \odot b) \oplus (a \odot c)$$

and the second equation follows trom commutativity of $\mathbb{T}$. However, not every element in $\mathbb{T}$ has an inverse with respect to $\oplus$: let $x \in \mathbb{R}$, then if $x$ were invertible, there would be a $y \in \mathbb{T}$ such that $x \oplus y = \min(x, y) = \infty$. But $\min(x, y)$ is either $y$ (if $y \leq x$) or $x$ (if $x < y \leq \infty$) for any $y \in \mathbb{T}$.
(b) $3 \odot (5 \oplus 7) = 3 + \min(5, 7) = 8$, $(3 \oplus -3)^2 = (3 \oplus -3) \odot (3 \oplus -3) = \min(3, -3) + \min(3, -3) = -6$, and $(1 \oplus 8)^4 = (1 \oplus 8) \odot (1 \oplus 8) \odot (1 \oplus 8) \odot (1 \oplus 8) = 4 \min(1, 8) = 4$.
(c) First note that for any $x, y \in \mathbb{R} \cup \{\infty\}$, one has $k \min(x, y) = \min(kx, ky)$. Writing out $(x \oplus y)^k$ means $k \min(x, y) = \min(kx, ky)$. On the other hand, $x^k \oplus y^k = \min(kx, ky)$. So the two expressions are equal.

**Problem 3.** (a) Prove that if $\varphi : R \to S$ is a ring isomorphism then $\varphi^{-1} : S \to R$ is a ring homomorphism, and hence also an isomorphism.
(b) Let $R$ be a ring and $I \subseteq R$ be an ideal and let $\varphi : R \to R/I$ be the canonical projection. Show that $\ker \varphi = I$ and $\varphi$ is a ring homomorphism.

**Solution.** (a) Firstly if $\varphi(1_R) = 1_S$ then $\varphi^{-1}(1_S) = 1_R$. If now $s_1, s_2 \in S$ then there exist a unique pair $r_1, r_2 \in R$ with $\varphi(r_1) = s_1$ and $\varphi(r_2) = s_2$. Then

$$\begin{aligned} \varphi^{-1}(s_1 + s_2) &= \varphi^{-1}(\varphi(r_1) + \varphi(r_2)) \\ &= \varphi^{-1}(\varphi(r_1 + r_2)) \\ &= r_1 + r_2 \\ &= \varphi^{-1}(s_1) + \varphi^{-1}(s_2). \end{aligned}$$

Also

$$\begin{aligned} \varphi^{-1}(s_1 s_2) &= \varphi^{-1}(\varphi(r_1)\varphi(r_2)) \\ &= \varphi^{-1}(\varphi(r_1 r_2)) \\ &= r_1 r_2 \\ &= \varphi^{-1}(s_1)\varphi^{-1}(s_2). \end{aligned}$$

Therefore $\varphi^{-1}$ is a homomorphism. Now since $\varphi$ is a bijection so too is $\varphi^{-1}$, and therefore $\varphi^{-1}$ is an isomorphism.
(b) Clearly we have $\varphi(1_R) = 1_R + I = 1_{R/I}$. If $r_1, r_2 \in R$ then

$$\begin{aligned}\varphi(r_1 + r_2) &= (r_1 + r_2) + I \\ &= (r_1 + I) + (r_2 + I) \\ &= \varphi(r_1) + \varphi(r_2),\end{aligned}$$

and

$$\begin{aligned}\varphi(r_1 r_2) &= (r_1 r_2) + I \\ &= (r_1 + I)(r_2 + I) \\ &= \varphi(r_1)\varphi(r_2).\end{aligned}$$

Finally, since $0_{R/I} = I$ and $r + I = I$ iff $r \in I$ we see that $r \in \ker\varphi \iff r + I = I \iff r \in I$. Therefore $\ker\varphi = I$.

**Problem 4.** Let $I$, $J$ and $K$ be ideals of a ring $R$. Show that

(a) $I \cap J$ and $IJ$ are ideals
(b) $IJ \neq I \cap J$,
(c) $I(J + K) = IJ + IK$,

**Solution.** (a) Since $I$ and $J$ are ideal, both contain 0, and thus $0 \in I \cap J$, and $I \cap J \neq \varnothing$. Assume that $x, y \in I \cap J$ and $r \in R$. Since $I$ and $J$ are both ideals, it follows that $x \pm y$ and $rx$ are in $I$ and in $J$. Thus $x \pm y$ and $rx$ are all in $I \cap J$. For the second assertion, note that $IJ$ contains all finite sums of products of elements of $I$ and $J$. Since $0 \in I$ and $0 \in J$, $0 = 0 \cdot 0 \in IJ$ and thus $IJ \neq \varnothing$. Let now $\sum_{i=1}^n x_i y_i$ and $\sum_{j=1}^m x'_j y'_j$ with $x_i, x'_j \in I$ and $y_j, y'_j \in J$. Then $\sum_{i=1}^n x_i y_i + \sum_{j=1}^m x'_j y'_j$ is clearly in $IJ$. If $r \in R$, then $r\left(\sum_{i=1}^n x_i y_i\right) = \sum_{i=1}^n (r x_i) y_i$ is also in $IJ$. Thus $IJ$ is an ideal.
(b) We need only show one example where the above is not true. Therefore consider $I = 2\mathbb{Z}$, $J = 4\mathbb{Z} \subseteq \mathbb{Z}$. Then $IJ = 8\mathbb{Z}$ but $I \cap J = 4\mathbb{Z}$.
(c) Choose $x \in I(J + K)$, then $x$ can be written as $\sum_{i=1}^n r_i(s_i + t_i)$ for some $n \in \mathbb{N}$, $r_i \in I$, $s_i \in J$ and $t_i \in K$. But then

$$\begin{aligned}x &= \sum_{i=1}^n (r_i s_i + r_i t_i) \\ &= \left(\sum_{i=1}^n r_i s_i\right) + \left(\sum_{i=1}^n r_i t_i\right) \\ &\in IJ + IK,\end{aligned}$$

so $I(J + K) \subseteq IJ + IK$. Conversely if $y \in IJ + IK$ then we can write $y = \sum_{i=1}^n r_i s_i + \sum_{j=1}^m r'_j t_j$ for some $n, m \in \mathbb{N}$, $r_i, r'_j \in I$, $s_i \in J$ and $t_j \in K$. Now

$$\begin{aligned}y = &\sum_{\substack{i \\ r_i = r'_j}} r_i(s_i + t_j) + \sum_{\substack{i \\ r_i \neq r'_j \forall j}} r_i(s_i + 0) + \sum_{\substack{j \\ r'_j \neq r_i \forall i}} r'_j(0 + t_j) \\ &\in I(J + K),\end{aligned}$$

so $IJ + IK \subseteq I(J + K)$ and therefore $IJ + IK = I(J + K)$.

**Problem 5.** Let $I$, $J$ and $K$ be ideals of a ring $R$. Recall that $(I : J) = \{r \in R : rJ \subseteq I\}$. Show that

(a) $(I : J)$ is an ideal of $R$ and $I \subseteq (I : J)$,
(b) $J \subseteq I$ implies that $(I : J) = R$,
(c) $IJ \subseteq K$ if and only if $I \subseteq (K : J)$.

**Solution.** (a) Clearly $0 \in (I : J)$ since $0J = \{0\} \subseteq I$. If $x_1, x_2 \in (I : J)$ then for all $y \in J$ we have $x_1y, x_2y \in I$, therefore $x_1y - x_2y = (x_1 - x_2)y \in I$. Hence $x_1 - x_2 \in (I : J)$. Finally if $x \in (I : J)$ and $r \in R$ then $rxJ \subseteq rI \subseteq I$, hence $rx \in (I : J)$.

If $x \in I$ and $y \in J$ then $xy \in I$, since $J \subseteq R$. Therefore $xJ \subseteq I$ and so $x \in (I : J)$ and $I \subseteq (I : J)$.
(b) If $J \subseteq I$ then $1J \subseteq I$, and $1 \in (I : J)$. But by part (a), $(I : J)$ is an ideal so $(I : J) = R$.
(c) Suppose first that $IJ \subseteq K$ and consider $x \in I$. Then for all $y \in J$ we have $xy \in IJ \subseteq K$, so $xJ \subseteq K$, i.e. $x \in (K : J)$ and $I \subseteq (K : J)$.

Conversely suppose $I \subseteq (K : J)$. Then $xy \in K$ for all $x \in I$ and $y \in J$. Hence all sums of the form $\sum_{i=1}^{n} x_i y_i$ with $n \in \mathbb{N}$, $x_i \in I$ and $y_i \in J$ are in $K$ also, and hence $IJ \subseteq K$.

**Problem 6.** Let $R$ be a commutative ring and let $I, J \subseteq R$ be ideals.

(a) Let $\sqrt{I} = \{r \in R : r^n \in I \text{ for some positive integer } n\}$. Show that $\sqrt{I}$ is an ideal that contains $I$. [Note: $\sqrt{I}$ is called the *radical of* $I$.]
(b) Prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
(c) Let $R = k[x, y]$. Show that $\sqrt{(x^2, y^2)} = (x, y)$ and that $\sqrt{(x^2) \cap (y^2)} = (xy)$.

(a) We have to show that $\sqrt{I}$ is closed under addition and multiplication in $R$. Let $x \in \sqrt{I}$, then there exists an integer $n > 0$ such that $x^n \in I$. If $r \in R$ then $(rx)^n = r^n x^n$ is contained in $I$ (since $I$ is an ideal in $R$). This means that $rx \in \sqrt{I}$. If $y$ is another element in $\sqrt{I}$, then there exists a $k > 0$ such that $y^k \in I$. Look at $(x + y)^{n+k}$. Use the binomial theorem:

$$(x+y)^{n+k} = \sum_{i=0}^{n+k} \binom{n+k}{i} x^i y^{n+k-i} = \underbrace{y^k \sum_{i=0}^{n-1} \binom{n+k}{i} y^{n+k-k-i} x^i}_{\in IR} + \underbrace{x^n \sum_{i=n}^{n+k} \binom{n+k}{i} y^{n+k-i} x^{i-n}}_{\in IR}$$

is contained in $I$. Thus $x + y \in \sqrt{I}$. Clearly $I \subseteq \sqrt{I}$, since for any $x \in I$, $x^1 \in \sqrt{I}$.
(b) First take $x \in \sqrt{I \cap J}$. This means that there exist $n > 0$ such that $x^n \in I$ and $x^n \in J$. This means that $x \in \sqrt{I}$ and $x \in \sqrt{J}$ and consequently in $\sqrt{I} \cap \sqrt{J}$. Now take $x$ in the intersection of the two radicals. This means that there exist $k, l > 0$ such that $x^k \in I$ and $x^l \in J$. Then $x^{k+l}$ is contained in both $I$ and $J$. Thus $x \in \sqrt{I \cap J}$.
(c) It is easy to see that $\sqrt{(x^2, y^2)} \supseteq (x, y)$. If $f(x, y)$ is an element in $k[x, y]$ such that for some $n > 0$, $f^n = ax^2 + by^2$, then $f$ cannot have a nonzero constant term. Thus $f$ must be of the form $f = cx + dy$ for some $c, d \in k[x, y]$. But this means that $f \in (x, y)$. For the second ideal use part (b): $\sqrt{(x^2) \cap (y^2)} = \sqrt{(x^2)} \cap \sqrt{(y^2)}$. Similar to the first ideal, one sees that $\sqrt{(x^2)} = (x)$ and $\sqrt{(y^2)} = (y)$, thus the ideal on the left hand side is $(x) \cap (y)$. Clearly $xy \in (x) \cap (y)$. For the other inclusion, if any $f(x, y) \in (x)$, then $f$ is a multiple of $x$, i.e., $f(x, y) = xg(x, y)$ for some $g(x, y) \in k[x, y]$. But then $xg(x, y) \in (y)$ if and only if $y$ is a factor of $xg(x, y)$, which means that $y$ has to be a factor of $g(x, y)$. Thus $f(x, y) \in (xy)$ and we have shown the equality $(x) \cap (y) = (xy)$.