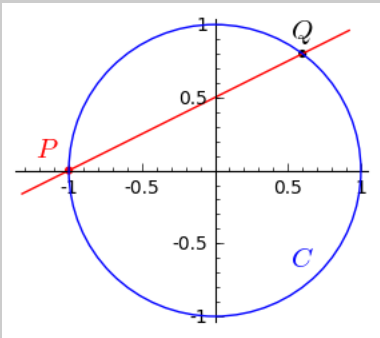
Problem class 1

1. A triple of natural number (X, Y, Z) is called a pythagorean triple if $X^2+Y^2 = Z^2$ as they are the sides of a triangle with a right angle. Consider $x = X/Z$ and $y = Y/Z$. Now we are looking for positive rational numbers x, y satisfying $x^2+y^2 = 1$. Use the ideas in Chapter 1 to find plenty of pythagorean triples.

Solution: The picture for $x^2+y^2 = 1$ is a circle C of radius 1 centred at the origin.



We pick the point $P = (-1, 0)$ as the starting point. Let L be a line through P; it can be given by equation $y = m(x + 1)$ for some slope m. The points in the intersection $C \cap L$ satisfy

$$\begin{aligned} x^2 + \big(m(x+1)\big)^2 &= 1 \\ (1+m^2)x^2 + 2m^2x + (-1+m^2) &= 0 \\ (x+1)\big((1+m^2)x + (-1+m^2)\big) &= 0 \end{aligned}$$

The first solution $x = -1$ corresponds to P. The second intersection Q has $x = (1-m^2)/(1+m^2)$. Plugging back into the line equation, we determine y by

$$y = m(x+1) = m\Big(\frac{1-m^2}{1+m^2} + 1\Big) = m\frac{1-m^2+1+m^2}{1+m^2} = \frac{2m}{1+m^2}$$

and hence

$$Q = (x, y) = \Big(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\Big).$$

For any $m \in \mathbb{Q}$ this gives a point on the circle and hence a pythaogrean triple. For instance, for any natural number m, the triple

$$X = m^2 - 1 \qquad Y = 2m \qquad Z = m^2 + 1$$

forms a triangle with a right angle. Here are a few examples:

$$(3, 4, 5),\ (8, 6, 10),\ (15, 8, 17),\ (24, 10, 26),\ (35, 12, 37),$$
$$(48, 14, 50),\ (63, 16, 65),\ (80, 18, 82),\ (99, 20, 101), \ldots$$

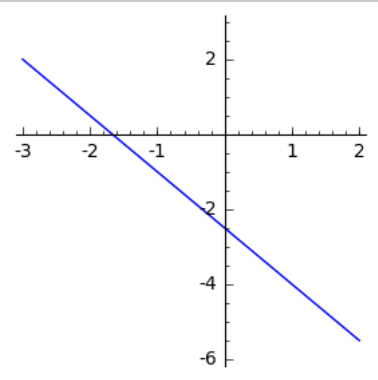
A different method is used in G13FNT=MATH3012

2. Draw a picture of the solution set $C(k)$ in k^2 for the equation

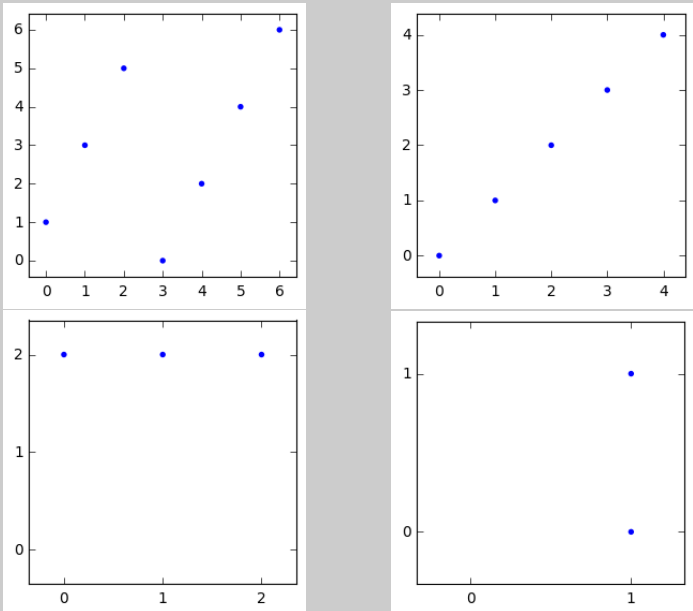
$$2\,y + 3\,x + 5 = 0$$

and the fields $k = \mathbb{R}$, $k = \mathbb{F}_7$, $k = \mathbb{F}_5$, $k = \mathbb{F}_3$, $k = \mathbb{F}_2$ and $k = \mathbb{Q}$.

Solution: The picture for $k = \mathbb{R}$ looks like a well-known line



For the finite fields, they look less like line even if we shall still think of them as lines. The four pictures for $p = 7$, $p = 5$, $p = 3$ and $p = 2$ in that order.



For $\mathbb{Q}$ it is hard to make a picture. If we print a small dot for each rational solution, the picture ends up looking exactly like the one for $\mathbb{R}$. Yet $C(\mathbb{Q})$ is much smaller than $C(\mathbb{R})$.

3. Let $(A, +)$ and $(B, \#)$ be abelian groups and let $f : A \to B$ be a map such that $f(-a) = -f(a)$ for all $a \in A$ and

$$a + a' + a'' = 0 \qquad \Rightarrow \qquad f(a)\#f(a')\#f(a'') = 0.$$

Prove that f is a group homomorphism.

Solution: Let a and a' be two elements in A. Set $a'' = -a - a' = -(a + a')$, then $a + a' + a'' = 0$. By the hypotheses $f(a)\#f(a')\#f(a'') = 0$, which implies that $f(a'') = -\big(f(a)\#f(a')\big)$. We conclude that $f(a + a') = -f\big(-(a + a')\big) = -f(a'') = f(a)\#f(a')$.

4. Let k be a field and $n > 0$. On the set $X = k^{n+1} \setminus \big\{(0, 0, \ldots, 0)\big\}$ define the following relation:

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n)$$
$$\text{if and only if there exists } \lambda \in k^\times \text{ such that}$$
$$x_0 = \lambda \cdot y_0,\ x_1 = \lambda \cdot y_1,\ \ldots,\ x_n = \lambda \cdot y_n$$

Prove that this is an equivalence relation. Recall, this means that we need to check

Reflexive: $a \sim a$ for all $a \in X$.

Symmetric: If $a \sim b$ for some $a, b \in X$ then $b \sim a$.

Transitive: If $a \sim b$ and $b \sim c$ for some $a, b, c \in X$, then $a \sim c$.

Solution:

Reflexive: $a \sim a$ is true by taking $\lambda = 1 \in k^\times$ in the definition.

Symmetric: If $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$, then there is a $\lambda \in k^\times$ such that $x_i = \lambda \cdot y_i$. Since λ is invertible, we find $y_i = \lambda^{-1} \cdot x_i$ for all $i = 0, \ldots, n$. This shows that $(y_0, \ldots, y_n) \sim (x_0, \ldots, x_n)$ as $\lambda^{-1} \in k^\times$.

Transitive: If $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ and $(y_0, \ldots, y_n) \sim (z_0, \ldots z_n)$ then there are $\lambda \in k^\times$ and $\mu \in k^\times$ such that $x_i = \lambda \cdot y_i$ and $y_i = \mu \cdot z_i$ for all $i = 0, \ldots, n$. Now $\lambda\mu \in k^\times$ and $x_i = \lambda\mu \cdot z_i$ shows that $(x_0, \ldots, x_n) \sim (z_0, \ldots, z_n)$.

Note that this proof also works for an arbitrary ring R and gives a definition of $\mathbb{P}^n(R)$ as long as we only allow vectors with at least one coordinate a unit in R and we only allow to scale through by invertible elements in $R^\times$.