Problem class 8

1. View ${}^{\mathbb{Q}^\times}/_{\square}$ as a vector space over $\mathbb{F}_2$. Determine the dimension of the subgroup generated by $\{6, -15, -10, 7\}$ when viewed as a subspace.

Solution: Probably the easiest is just to list all elements of this subspace W (with all equalities in ${}^{\mathbb{Q}^\times}/_{\square}$):

$$W = \{1,\ 6,\ -15, 6\cdot(-15) = -10,\ -10,\ 6\cdot(-10) = -60,\ (-15)\cdot(-10) = 6,$$
$$(-10)\cdot(-10) = 1,\ 7,\ 7\cdot 6 = 42,\ 7\cdot(-15) = -105,\ \dots\}$$

Hence $W = \{1, 6, -15, -10, 7, 42, -105, -70\}$. Since there are 8 elements the dimension is 3 as $2^3 = 8$.

Alternatively, we can view the set $\{-1, 2, 3, 5, 7, 11, \dots\}$ consisting of -1 and all primes as a basis of ${}^{\mathbb{Q}^\times}/_{\square}$ as every vector in ${}^{\mathbb{Q}^\times}/_{\square}$ can be written uniquely as a finite linear combination of basis vectors. In that basis the four elements generating W are written as

$$\begin{aligned} 6 &= (0,1,1,0,0,0,\dots) \\ -15 &= (1,0,1,1,0,0,\dots) \\ -10 &= (1,1,0,1,0,0,\dots) \\ 7 &= (0,0,0,0,1,0,\dots) \end{aligned}$$

Clearly the first three are linearly dependent, i.e. $6\cdot(-15)\cdot(-10)$ is a square. Instead 6, -15, 7 are linearly independent and they form a basis of W. Hence the dimension is 3.

2. Let E be an elliptic curve over $\mathbb{Q}$ of the form $y^2 = (x-e_1)(x-e_2)(x-e_3)$ and let κ be the Kummer map. Show that the image of κ is contained in the subgroup $\big\{(a,b,c) \bigm| abc = \square\big\}$ of ${}^{\mathbb{Q}^\times}/_{\square} \times {}^{\mathbb{Q}^\times}/_{\square} \times {}^{\mathbb{Q}^\times}/_{\square}$.

Solution: Assume first that $P = (x_P, y_P)$ is not a 2-torsion point. Then $\kappa(P) = (a,b,c)$ with $a = (x_P - e_1)\cdot\square$, $b = (x_P - e_2)\cdot\square$ and $c = (x_P - e_3)\cdot\square$. Therefore

$$abc = (x_P - e_1)(x_P - e_2)(x_P - e_3)\cdot\square = y_P^2\cdot\square = \square.$$

If $P = O$ the statement is obvious. For $P = (e_1, 0)$ we get $\kappa\big((e_1,0)\big) = (a,b,c)$ with $a = (e_1-e_2)(e_1-e_3)\cdot\square$, $b = (e_2 - e_1)$ and $c = (e_1 - e_3)\cdot\square$. Hence $abc = (e_1-e_2)(e_1-e_3)(e_2-e_1)(e_3-e_1)\cdot\square = \big((e_1-e_2)(e_1-e_3)\big)^2\cdot\square = \square$. The cases $(e_1,0)$ and $(e_3,0)$ are similar.

3. Let $E : y^2 = (x+4)(x+1)(x-5)$ which contains the following rational points

$$T_1 = (-4,0) \qquad T_2 = (-1,0) \qquad T_3 = (5,0)$$
$$P_1 = (-3,4) \qquad P_2 = (8,18) \qquad P_3 = (23,108)$$

Compute the image under the Kummer map of all these six points. Prove that the image of these six points generate a group isomorphic to $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. Use it to find relations among the points.

Solution: The following table lists the values of the Kummer map. All elements in $\mathbb{Q}^\times/\square$ are written as the unique non-zero square-free integer in the coset.

P	$\kappa_1(P)$	$\kappa_2(P)$	$\kappa_3(P)$
$T_1 = (-4,0)$	3	-3	-1
$T_2 = (-1,0)$	3	-2	-6
$T_3 = (5,0)$	1	6	6
$P_1 = (-3,4)$	1	-2	-2
$P_2 = (8,18)$	3	1	3
$P_3 = (23,108)$	3	6	2

Since $T_1 + T_2 = T_3$, but they all have all distinct values in the image, we have already a copy of $\left(\mathbb{Z}/2\mathbb{Z}\right)^2$ present in the image. The point P_1 maps outside of these four points, so the points T_1, T_2 and P_1 generate a group isomorphic to $\left(\mathbb{Z}/2\mathbb{Z}\right)^3$. We only need to check now that the other two points map into that group, too. Indeed we have $\kappa(P_1)\cdot\kappa(T_2) = (1,-2,-2)\cdot(3,-2,-6) = (3,1,3) = \kappa(P_2)$ and $\kappa(P_1)\cdot\kappa(T_1) = (1,-2,-2)\cdot(3,-3,-1) = (3,6,2) = \kappa(P_3)$. By the way, the two missing elements of the group generated by the image of the six points are $\kappa(O) = (1,1,1)$ and $\kappa(P_1+T_3) = (1,-3,-3)$.

We compute $P_1 + T_2 = (8,18) = P_2$ and $P_1 + T_1 = (23,-108) = -P_3$ which are are together with $T_1 + T_2 = T_3$ all the relations among the six points. By the way, the eighth point in the group generated by these six point in $E(\mathbb{Q})/2E(\mathbb{Q})$ is $P_1 + T_3 = \left(-\frac{7}{4}, -\frac{27}{8}\right)$.

4. Let E be an elliptic curve over $\mathbb{R}$ with positive discriminant Δ. We know that we can write it as $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1 < e_2 < e_3$. Determine the Kummer map $\kappa\colon E(\mathbb{R}) \to \mathbb{R}^\times/\square \times \mathbb{R}^\times/\square \times \mathbb{R}^\times/\square$ and conclude that

$$2\,E(\mathbb{R}) = \{O\} \cup \left\{(x_P, y_P) \in E(\mathbb{R}) \;\middle|\; x_P \geqslant e_3\right\}.$$

Solution: First note that $\mathbb{R}^\times/\square \cong \{1,-1\}$ only remembers the signs of the non-zero real number. Using $e_1 < e_2 < e_3$ for the three torsion points we find

$$\kappa\big((e_1,0)\big) = (1,-1,-1) \text{ and } \kappa\big((e_2,0)\big) = (1,-1,-1) \text{ and } \kappa\big((e_3,0)\big) = (1,1,1).$$

If $x < e_1$ or if $e_2 < x < e_3$ then $(x - e_1)(x - e_2)(x - e_3) < 0$ and hence there is no point with this x-coordinate. Therefore, if $P = (x_P, y_P)$, then either $e_1 \leqslant x_P \leqslant e_2$ or $e_3 \leqslant x_P$. If $e_1 < x_P < e_2$, then $\kappa(P) = (1, -1, -1)$, otherwise $\kappa(P) = (1, 1, 1)$. Therefore $2\,E(\mathbb{R}) = \ker \kappa$ consists of all P with $x_P \geqslant e_3$ or $P = O$.