1 Solutions of First Assignment

1. (a) In the projective plane $\mathbb{P}^2$ we are given the points $(1:0:0), (0:1:0), (0:0:1), (1:1:1)$. Determine all projective curves of degree 2 which pass through these points.

   Solution: The general conic C is given by

   $$ax^2 + by^2 + cz^2 + dxy + exz + fyz = 0$$

   with a, b, c, d, e, f not all zero. The assumption that C contains $(1:0:0)$ gives us that $a = 0$. Similarly, $b = c = 0$. Finally the condition $(1:1:1) \in C$ yields $d + e + f = 0$. Hence, the general form is

   $$d(xy - yz) + e(xz - yz) = 0.$$

   (b) Given any five points in $\mathbb{P}^2$. Show that there exists a curve of degree 2 passing through these points.

   Solution: Take again the conic with general coefficients a, b, c, d, e, f. The condition that a given point lies on it yields one homogeneous linear equation for a, b, c, d, e, f. So five points give us five linear homogeneous equations. Since the number of unknowns is six, there must be a non-trivial solution for a, b, c, d, e, f by linear algebra.

   (c) Suppose that among five points in $\mathbb{P}^2$ there are three points on a straight line. Show that any quadratic curve through the five points is a union of to straight lines.

   Solution: Let l be the straight line and let C be a conic through the five points. Then C and l have at least three points of intersection. By Bezout's theorem, this is not possible if C and l have no component in common. Hence l is contained in C.

2. In this problem we determine the solutions of

   $$(xy + xz + yz)^2 - 4xyz(x + y + z) = 0 \qquad \text{(C)}$$

   in $x, y, z \in \mathbb{Z}$. Consider the projective curve C given by this equation.

   (a) Show that the points $(1:0:0), (0:1:0), (0:0:1)$ are singular points of C.

   Solution: Let F be the left hand side of (C). The partial derivatives of F read

   $$\begin{aligned} F_x &= 2(xy + xz + yz)(y + z) - 4yz(x + y + z) - 4xyz \\ F_y &= 2(xy + xz + yz)(x + z) - 4xz(x + y + z) - 4xyz \\ F_z &= 2(xy + xz + yz)(x + y) - 4xy(x + y + z) - 4xyz \end{aligned}$$

   One easily verifies that these are zero in the three given points.

(b) Prove that these are the only singular points.

Solution: We solve the system $F_x = F_y = F_z = 0$ (see previous item). There are many way to solve this system, some are complicated, some are simple. We give the shortest one here. Notice that $F_x + F_y + F_z = -12xyz$. Hence at least one of x, y, z is zero. Let us take $x = 0$. We obtain $F_y = 2yz^2 = 0$, which implies $y = 0$ or $z = 0$. So we recover the points $(0 : 1 : 0)$ and $(0 : 0 : 1)$. When we start with $y = 0$ or $z = 0$ the computation runs similarly.

(c) Consider the family of quadratic curves Q_t given by the projective equation

$$xy + t(x - y)z = 0$$

with parameter t. Show that every curve Q_t passes through the singular points of C and determine the points of intersection between C and Q_t for every t.

Solution: Since the equation for Q_t does not contain terms x^2, y^2 or z^2, it contains the points $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$. (An instructional side remark: since these are singular points of C, these points of intersection already account for intersection multiplicity $2+2+2 = 6$. By Bezout, the total intersection multiplicity is eight. Furthermore in the point $(0 : 0 : 1)$ the curve Q_t has a tangent conciding with one of the 'tangents' of C. This accounts for one more intersection point. There is now essentially one point left to compute).

Let us do the computation. To make things easier, set $z = 1$. The curve Q_t reads

$$y = tx/(t - x)$$

which we substitute in the affine equation for C : $(xy+x+y)^2-4xy(x+y+1) = 0$. We get

$$\left(\frac{tx(x+1)}{t-x} + x\right)^2 - \frac{4tx^2}{t-x}\left(x + \frac{tx}{t-x} + 1\right) = 0.$$

Multiply by $(t - x)^2$ and simplify to obtain

$$((t-1)x^2 + 2tx)^2 - 4tx^2(-x^2 + (2t-1)x + t) = 0.$$

Divide by x^2 (we ignore the intersection point with $x = 0$ which we already know) and simplify to get

$$(t+1)^2x^2 - 4t^2x = 0.$$

Divide by x and we obtain $x = 4t^2/(t+1)^2$ and hence $y = 4t^2/(t-1)^2$. So we see that we can parametrize C rationally. In homogeneous coordinates,

$$(x : y : z) = (4t^2(t-1)^2 : 4t^2(t+1)^2 : (t^2-1)^2).$$

To every point on C there corresponds the parameter $t = xy/(y - x)$ from the equation of Q_t.

(d) Determine a rational parametrisation of C. Then prove that the full solution set of (C) is given by the integer multiples of the solutions of the form

$$(a^2b^2, (a-b)^2a^2, (a-b)^2b^2)$$

where $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$.

Solution: The rational parametrization is already given. Suppose now we have an integer solution $(x0 : y0 : z0)$ and suppose for the moment that $\gcd(x0 : y0 : z0) = 1$. From the parametrisation we know that there exists $t \in \mathbb{Q}$ such that

$$(x0 : y0 : z0) = (4t^2(t-1)^2 : 4t^2(t+1)^2 : (t^2-1)^2)$$

Put $t = r/s$ with $r, s \in \mathbb{Z}$. Then

$$(x0 : y0 : z0) = (4r^2(r-s)^2 : 4r^2(r+s)^2 : (r^2-s^2)^2).$$

Now put $a = 2r, b = r - s$. Then

$$(x0 : y0 : z0) = (a^2b^2 : a^2(a-b)^2 : (a^2-b^2)^2).$$

Replace a, b by $a/\gcd(a, b)$ and $b/\gcd(a, b)$ and we get a solution with relatively prime coordinates which are eqqual to $x0, y0, z0$ up to common ± 1 factor. Any other solution is an integer multiple of such a relatively prime solution.

(e) (Bonus problem) Consider the diophantine equation

$$(xy + xz + yz)^2 - 3xyz(x + y + z) = 0.$$

So the 4 in equation (C) changed into 3. Prove or disprove the following claim: all solutions $x, y, z \in \mathbb{Z}$ are given by integer scalar multiples of $(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)$.

Solution: Observe that $(xy + xz + yz)^2 - 3xyz(x + y + z)$ equals $x^2y^2 + x^2z^2 + y^2z^2 - xyz^2 - xy^2z - x^2y$ which equals

$$\frac{1}{2}(xy - xz)^2 + \frac{1}{2}(xz - yz)^2 + \frac{1}{2}(xz - yz)^2,$$

hence the sum of squares. This can only be zero if $xy - xz = xz - yz = xz - yz = 0$. It then follows that the four solutions mentioned are the only ones.

3. We consider the algebraic number field $K = \mathbb{Q}(\zeta_5)$ where ζ_5 is a non-trivial fifth root of unity (e.g. $\zeta_5 = e^{2\pi i/5}$).

(a) Determine the minimal polynomial for ζ_5. Then determine the number of real and the number of complex embeddings of K.

Solution: This is more or less standard, ζ_5 satisfies $x^5 - 1$ and since $\zeta_5 \neq 1$ it is also zero of $\frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$. It then needs to be shown that $x^4+x^3+x^2+x+1$ is irreducible. Since the zeros of $x^4 + x^3 + x^2 + x + 1$ are ζ_5^k for $k = 1, 2, 3, 4$, all complex, there are no real embeddings. Hence $r_1 = 0, r_2 = 2$.

(b) Show that the following elements of K are algebraic integers,

$$\zeta_5,\ u_k = \frac{1-\zeta_5^k}{1-\zeta_5},\ 1/u_k = \frac{1-\zeta_5}{1-\zeta_5^k}$$

where k is any integer not divisible by 5. Thus we can conclude that u_k is a unit in the integers of K for all $k = 1, 2, 3, 4$ (cyclotomic units).

Solution: Clearly ζ_5 is an integer because its minimal polynomial has integer coefficients. Notice that $\frac{1-\zeta_5^k}{1-\zeta_5} = 1 + \zeta_5 + \cdots + \zeta_5^{k-1}$ is also an integer. Given k there exists an integer l such that $lk \equiv 1 (\text{mod } 5)$. Then observe that

$$\frac{1-\zeta_5}{1-\zeta_5^k} = \frac{1-\zeta_5^{kl}}{1-\zeta_5^k} = 1 + \zeta_5^k + \cdots + \zeta_5^{(l-1)k}.$$

The latter number is an integer. Hence $(1-\zeta_5^k)/(1-\zeta_5)$ is a unit.

(c) Prove that $5 = \prod_{k=1}^4 (1-\zeta_5^k)$. Then show that there is unit u in the integers of K such that $5 = u(1-\zeta_5)^4$.

Solution: We know that $x^4 + x^3 + x^2 + x + 1 = \prod_{k=1}^4 (x - \zeta_5^k)$. Setting $x = 1$ gives us $5 = \prod_{k=1}^4 (1-\zeta_5^k)$. We have seen above that there exist units u_k such that $1 - \zeta_5^k = u_k(1-\zeta_5)$. Hence $5 = u_2 u_3 u_4 (1-\zeta_5)^4$.

(d) Show that $\zeta_5^2 + \zeta_5^{-2} = -\eta$, where η is the golden ratio $\eta = (1+\sqrt{5})/2$. Hence $\mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{Q}(\zeta_5)$.

Solution: Note that $(\zeta_5^2 + \zeta_5^{-2})^2 + (\zeta_5^2 + \zeta_5^{-2})$ equals

$$\zeta_5^4 + \zeta_5^{-4} + 2 + \zeta_5^2 + \zeta_5^{-2} = 2 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 1.$$

Hence our number is a zero of $x^2 + x - 1$. The solution are $(-1 \pm \sqrt{5})/2$. Since our number has negative real part we must pick $(-1-\sqrt{5})/2 = -\eta$.

(e) Let α be an integer in $\mathbb{Q}(\sqrt{5})$ and let α' be its conjugate. Show that if $\alpha \neq 0, \pm 1$ then $\max(|\alpha|, |\alpha'|) \geq \eta$.

Solution: An integer in $\mathbb{Q}(\sqrt{5})$ has the form $(a + b\sqrt{5})/2$ with $a, b \in \mathbb{Z}$ and $a \equiv b (\text{mod } 2)$. Suppose that a, b have the same sign. Then $|(a+b\sqrt{5})/2| = |a|/2 + |b|\sqrt{5}/2$. When $a = 0$ we have b even (and non-zero by assumption) and our absolute value exceeds $\sqrt{5} > \eta$. When $b = 0$ we have a even (and $\neq 0, \pm 2$ by assumption) and our absolute value exceeds $2 > \eta$. When both $|a|, |b| \geq 1$ our inequality follows trivially. When a, b have opposite sign we can apply our argument to $|\alpha'|$ instead.

(f) Use Dirichlet's theorem for units in $\mathbb{Q}(\zeta_5)$ and the lower bound just given to show that the unit group of the integers in $\mathbb{Q}(\sqrt{5})$ are given by $\pm\eta^k$ with $k \in \mathbb{Z}$.

Solution: We know that $r_1 = 2, r_2 = 0$. The roots of unity are ± 1 (we are in a real field). By Dirichlet's Theorem there exists a unit u such that the group of units is generated by u and -1. We know that η is unit, hence there exists $k \in \mathbb{Z}$ such

that $\eta = \pm u^k$. By replacing u by its conjugate if necessary, we can assume that $k > 0$ and $|u| > 1$. From the previous exercise we know that $|u| \geq \eta$. Hence $k = 1$ and we see that η is a generator of the unit group.

(g) Prove that the roots of unity in $\mathbb{Q}(\sqrt{5})$ are given by $\pm\zeta_5^k$ with $k = 0, 1, 2, 3, 4$.

Solution: This is not so easy. The Galois group of $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is generated by one element σ of order 4 with the property that $\sigma(\zeta_5) = \zeta_5^2$. Moreover, $\sigma(\sqrt{5}) = -\sqrt{5}$. Let $u \in \mathbb{Q}(\sqrt{5})$ be a root of unity. Then $u + 1/u$ is in the real subfield $\mathbb{Q}(\sqrt{5})$. It is also an integer in that field, so $u + 1/u = (a + b\sqrt{5})/2$ with $a, b \in \mathbb{Z}$ and $a \equiv b (\mathrm{mod}\ 2)$. Since $|u| = 1$ we know that $|u + 1/u| \leq 2$. Apply σ and we get that $\sigma(u) + 1/\sigma(u) = (a - b\sqrt{5})/2$. Since $\sigma(u)$ is also a root of unity we get $|a - b\sqrt{5}|/2$. From these inequalities it follows that $u + 1/u$ is one of $0, \pm 1, \pm 2, (\pm 1 \pm \sqrt{5})/2$. Solving $u + 1/u = 0, \pm 1$ gives us that u is a fourth or cube root of unity, which is not possible in $\mathbb{Q}(\zeta_5)$. The other possibilities give us the ten roots of unity $\pm\zeta_5^k$.

(h) Prove that if u is a unit in $\mathbb{Q}(\zeta_5)$ then $u\overline{u}$ is a unit in $\mathbb{Q}(\sqrt{5})$ ($\overline{u}$ is the complex conjugate of u). Determine $u_2\overline{u}_2$ where $u_2 = 1 + \zeta_5$.

Solution: If u is a unit, then $\overline{u}$ is also a unit, as well as the product $|u|^2 = u\overline{u}$. Moreover, $|u|^2$ lies in the real subfield of $\mathbb{Q}(\zeta_5)$, which is $\mathbb{Q}(\sqrt{5})$. Notice that

$$|u_2|^2 = (1 + \zeta_5)(1 + \zeta_5^{-1}) = 2 + \zeta_5^2 + \zeta_5^{-2} = 2 - \eta.$$

(i) Use Dirichlet's theorem and the previous problems to prove that the group of units in $\mathbb{Q}(\zeta_5)$ is given by $\pm\zeta_5^k(1 + \zeta_5)^l$, $k = 0, 1, 2, 3, 4; l \in \mathbb{Z}$.

Solution: Since $r_1 = 0, r_2 = 2$, the group of units is generated by $-\zeta_5$ and a fundamental unit u. There exists $k \in \mathbb{Z}$ such that $\eta = \zeta u^k$ where ζ is a root of unity. Let us assume $|u| > 1$. Taking absolute values, $|u|^{2k} = \eta^2$. We also know that $|u|^2$, being an integer in $\mathbb{Q}(\sqrt{5})$, is at least η. Hence $k = 1$ or 2. When $k = 1$ we have that u equals η up to root of unity. So let us suppose that $k = 2$. Without loss of generality we can assume that $\zeta = \pm 1$. Hence $\eta = \pm u^2$. Clearly, u cannot be real because then $u \in \mathbb{Q}(\sqrt{5})$. Hence $\eta = -u^2$. Apply σ, $\sigma(\eta) = -\sigma(u)^2$. Since $\sigma(\eta) = (1 - \sqrt{5})/2 < 0$ we see that $\sigma(u)$ must be real and we again have a contradiction.

Thus we conclude that the unit group is generated by the roots of unity and η. Our assertion now follows because $1 + \zeta_5 = \zeta_5^2(\zeta_5^2 + \zeta_5^{-2}) = -\zeta_5^2\eta$

4. We solve the diophantine equation $x^2 - 2y^2 = z^3$ in $x, y, z \in \mathbb{Q}$ and in integers x, y, z with $\gcd(x, y) = 1$.

(a) Choose $r, s \in \mathbb{Q}$ arbitrarily. Show that $x = r(r^2 - 2s^2), y = (r^2 - 2s^2)s, z = r^2 - 2s^2$ is a rational solution of our equation. Prove that any rational solution of $x^2 - 2y^2 = z^3$ is of this form.

Solution: Let x, y, z be any rational solution. Put $r = x/z$ and $s = y/z$. From our equation we get $z = (x/z)^2 - 2(y/z)^2 = r^2 - 2s^2$. So $z = r^2 - 2s^2$ from which $x = rz = r(r^2 - 2s^2)$ and $y = sz = s(r^2 - 2s^2)$ follow immediately.

(b) Let $x, y, z \in \mathbb{Z}$ be a solution of $x^2 - 2y^2 = z^3$ with $\gcd(x, y) = 1$. Prove that x is odd.

Solution: Suppose that x is even. Then, from our equation, it follows that z is even. But then $2^2 = 4$ divides $2y^2$. Hence y is even, which contradicts our requirement that $\gcd(x, y, z) = 1$.

(c) We are given that $\mathbb{Z}[\sqrt{2}]$ is a unique factorization domain and its unit group is given by $\pm(-1 + \sqrt{2})^k$, $k \in \mathbb{Z}$. By factorization of $x^2 - 2y^2$ over $\mathbb{Z}[\sqrt{2}]$ solve the equation $x^2 - 2y^2 = z^3$ in integers x, y, z with $\gcd(x, y) = 1$.

Solution: Consider the factorization

$$(x + y\sqrt{2})(x - y\sqrt{2}) = z^3.$$

Suppose we have a prime $\pi \in \mathbb{Z}[\sqrt{2}]$ which divides both $x \pm y\sqrt{2}$. Then π divides $2x$ and $2y\sqrt{2}$. Since $\gcd(x, y) = 1$ this implies that π divides $\sqrt{2}$. But then it follows from $\pi | x + y\sqrt{2}$ that x is even, which is not possible. Thus we see that $x \pm y\sqrt{2}$ are relatively prime. Hence it follows from unique factorization in $\mathbb{Z}[\sqrt{2}]$ that $x + y\sqrt{2} = \epsilon\alpha^3$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$ and ϵ a unit. Modulo cubes ϵ is equal to one of $1, 1 + \sqrt{2}$ or $1 + \sqrt{2}$ (its inverse power). Put $\alpha = r + s\sqrt{2}$ with $r, s \in \mathbb{Z}$. Then we obtain three cases,

$$\begin{aligned}
x + y\sqrt{2} &= (r + s\sqrt{2})^3 = r^3 + 6rs^2 + (3r^2s + 2s^3)\sqrt{2} \\
x + y\sqrt{2} &= (-1 + \sqrt{2})(r + s\sqrt{2})^3 \\
&= -r^3 + 6r^2s - 6rs^2 + 4s^3 + (r^3 - 3r^2s + 6rs^2 - 2s^3)\sqrt{2} \\
x + y\sqrt{2} &= (1 + \sqrt{2})(r + s\sqrt{2})^3 \\
&= r^3 + 6r^2s + 6rs^2 + 4s^3 + (r^3 + 3r^2s + 6rs^2 + 2s^3)\sqrt{2}
\end{aligned}$$

Notice that the latter two solution types are related by $s \to -s$. So the full solution set reads

$$x = r^3 + 6rs^2, \quad y = 3r^2s + 2s^3$$

and

$$x = \pm(r^3 + 6r^2s + 6rs^2 + 4s^3), \quad y = r^3 + 3r^2s + 6rs^2 + 2s^3.$$

Strictly speaking one would have to verify for which choices of r, s the values of x, y are relatively prime (answer: $\gcd(r, s) = 1$ and r odd).