Assignment-2

Algebraic Geometry

Trishan Mondal, Soumya Dasgupta, Aaratrick Basu

Chapter 1

Problem 2.1. *Parametrise the conic $C : (x^2 + y^2 = 5)$ by considering a variable line though $(2, 1)$ and hence find all rational solutions of $x^2 + y^2 = 5$.*

Solution. Let ℓ be any line through the point $(2, 1)$ with slope t, then equation of ℓ is given by

$$y = t(x - 2) + 1.$$

Now we know that ℓ intersects the conic $C : x^2 + y^2 - 5 = 0$ at two points one of which is $(2, 1)$, to find the other point we substitute $y = t(x - 2) + 1$ in the equation $x^2 + y^2 - 5 = 0$, we get that

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

Since 2 is already a root of this equation we get the other root to be

$$x_t = \frac{2(t^2 - t - 1)}{1 + t^2} \Rightarrow y_t = \frac{-t^2 - 4t + 1}{1 + t^2}.$$

This gives us a bijection from $\varphi : (C \setminus \{(2, 1)\}) \cap (\mathbb{Q} \times \mathbb{Q}) \to \mathbb{Q}$, as follows,

$$\varphi(x, y) = \frac{y - 1}{x - 2}.$$

With the inverse map given by $\varphi^{-1}(t) = \left(\frac{2(t^2-t-1)}{1+t^2}, \frac{-t^2-4t+1}{1+t^2}\right)$. Thus we get all the rational solutions of $x^2+y^2 = 5$ are $\left\{\left(\frac{t^2-t-1}{1+t^2}, \frac{-t^2-4t+1}{1+t^2}\right) \mid t \in \mathbb{Q}\right\} \cup \{(2, 1)\}$.

Problem 2.2. *Let p be a prime, by experimenting with various p, guess a necessary and sufficient condition for $x^2+y^2 = p$ to have rational solutions; prove your guess.*

Solution. We claim that $x^2 + y^2 = p$, has a rational solution if and only if p is prime of the form $4k + 1$. From elementary number theory we know that if $p = 4k + 1$ for some k, then there exists integer a, b such that $a^2 + b^2 = p$, thus in this case $x^2 + y^2 = p$ has a rational solution.

Conversely suppose $x^2 + y^2 = p$ has a rational solution, let $x = \frac{a}{b}$ and $y = \frac{c}{d}$ with $\gcd(a, b) = \gcd(c, d) = 1$. Then we get that

$$(ad)^2 + (cb)^2 = p(bd)^2.$$

Now let q be a prime dividing b say $q^\alpha \mid b$, then from $(ad)^2 = b^2(pd^2 - c^2)$ we get that $q^\alpha \mid ad$, but $q \nmid a$, hence $q^\alpha \mid d$. Similarly we get that if r is prime divisor of d, say $r^\beta \mid d$, then $r^\beta \mid b$. Thus we can say that $b = \pm d$. Hence we get that

$$a^2 + c^2 = pb^2$$

Now if $p \mid c$, then we must have $p \mid a$, which in fact implies that $p \mid b$ (contradiction!), thus we must have $p \nmid c$ and $p \nmid a$. But then let $s = ac^{-1}$ modulo p, then $s^2 = -1$ modulo p. Thus the group $\mathbb{F}_p^*$ has an element of order 4. Thus we get that

$$4 \mid |\mathbb{F}_p^*| = p - 1 \Rightarrow p = 4k + 1.$$

Hence, we have proved that $x^2 + y^2 = p$ has a rational solution if and only if $p = 4k + 1$ prime.

Problem 2.3. *Let $P_1, \ldots, P_4$ be distinct points of $\mathbb{P}^2$ with no 3 collinear. Prove that there is a unique coordinate system in which the 4 points are $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$. Find all conincs passing through $P_1, \ldots, P_5$ where $P_5 = (a,b,c)$ is some other point, and use this to give another proof of Corollary 1.10 and Corollary 1.11.*

Solution. Note that since no three of P_1, P_2, P_3 and P_4 are collinear in $\mathbb{P}_k^2$ (we fix a representation in k^3 for all of these points), we get that as points in k^3 any three of them are linearly independent. And we can always find $u_1, u_2, u_3 \in k \setminus \{0\}$ such that

$$P_4 = u_1 P_1 + u_2 P_2 + u_3 P_3.$$

None of u_1, u_2, u_3 can be 0, because otherwise the other three points would be collinear in $\mathbb{P}_k^2$. Now there exists an unique linear map $T : k^3 \to k^3$ such that $T(P_i) = \frac{1}{u_i}\mathbf{e}_i$ for $i = 1, 2, 3$. Then observe that $T(P_4) = (1,1,1)$. Now since $T(\lambda x) = \lambda T(x)$, we get that T induces a map from $\mathbb{P}_k^2 \to \mathbb{P}_k^2$ such that $T(P_i) = [\mathbf{e}_i]$ for $i = 1, 2, 3$ and $T(P_4) = [1, 1, 1]$. Hence, we have proved that there exists a unique coordinate system in which the 4 points are $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$.

Conics passing through $P_1, \ldots, P_5$ where $P_5 = (a,b,c)$. Let $Q = Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2$ represent a conic passing through $P_1, \ldots, P_5$, then plugging in all the points, we get that

$$\begin{aligned}
&A = C = F = 0 \text{ and} \\
&B + D + E = 0 \text{ and } B(ab) + D(ac) + E(bc) = 0.
\end{aligned}$$

But then note that $B + D + E = 0$ and $B(ab) + D(ac) + E(bc) = 0$ defines a two planes, and the in order to find all the conics passing through $P_1, \ldots, P_5$ its sufficient to find the points in the intersection of the two planes. And it is obvious that the intersection of the two planes $\pi_1 : B + D + E = 0$ and $\pi_2 : B(ab) + D(ac) + E(bc) = 0$, is either a line (i.e., a one dimensional vector space) or a plane (when $(ab, ac, bc) = \lambda(1,1,1)$ for some $\lambda \in k$).

Proof of Corollary 1.10. Note that if $(ab, ac, bc) = \lambda(1,1,1)$ and $\lambda \neq 0$, then we get that $a = b = c$, hence $(a,b,c) = P_4$ in $\mathbb{P}_k^2$. On the other hand if $\lambda = 0$, at least two among a, b, c is zero, and since $(a,b,c) \in \mathbb{P}_k^2$, the other coordinate has to be nonzero, hence in this case $(a,b,c) \in \{P_1, P_2, P_3\}$.

Hence if $P_5 \notin \{P_1, \ldots, P_4\}$ (i.e., none of the fours points $P_1, \ldots, P_5$ are collinear), we get that the intersection of the two planes π_1 and π_2 is a line, i.e., a one dimensional vector space, hence we can conclude that

$$\dim S_2(P_1, \ldots, P_5) = 1.$$

Thus we have proved that if $P_1, \ldots, P_5 \in \mathbb{P}_k^2$ are distinct points and no 4 are collinear, there exists exactly one conic through $P_1, \ldots, P_5$ (which completes the proof of Corollary 1.10).

Proof of Corollary 1.11. Using Corollary 1.10, we can say that

$$1 = \dim S_2(P_1, \ldots, P_5) \geq \dim S_2(P_1, \ldots, P_n) - (5 - n)$$

since each point imposes at most one linear condition, hence we get that

$$\dim S_2(P_1, \ldots, P_n) \leq 6 - n,$$

From the previous proposition we have seen $\dim S_2(P_1, \ldots, P_n) \geq 6 - n$, so we get equality. which completes the proof of Corollary 1.11.

Problem 2.4. *In* (1.12) *there is a list of possible ways in which two conics can intersect. Write down the equations showing that each possiblity really occurs. Find all the singular conics in the corresponding pencils.*

Problem 2.5. *Let k be an algebraically closed field, and suppose given a quadratic and cubic form in U, V as in (1.8):*

$$q(U,V) = a_0U^2 + a_1UV + a_2V^2$$
$$c(U,V) = b_0U^3 + b_1U^2V + b_2UV^2 + b_3V^3.$$

Prove that q and c have a common zero $(\eta : \tau) \in \mathbb{P}^1$ if and only if

$$\det \begin{vmatrix} a_0 & a_1 & a_2 & & \\ & a_0 & a_1 & a_2 & \\ & & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & \\ & b_0 & b_1 & b_2 & b_3 \end{vmatrix} = 0$$

We will show that q and c has a common factor if and only if there exists homogeneous polynomials r and s with degree 2 and 1 respectively such that $rq + sc = 0$.

If there exists a common root $[\eta, \tau] \in \mathbb{P}$ of q and c, WLOG assume that $\tau \neq 0$ (the case when $\eta \neq 0$ can be tackled similarly), then $[\alpha, 1] \in \mathbb{P}^1_k$ is a common root of q and c. Thus we get that $q(U,V) = (U - \alpha V)q_1(U,V)$ and $c(U,V) = (U-\alpha V)c_1(U,V)$ were q_1 and c_1 are non-zero polynomials. Then we can take $r = c_1$ and $s = -q_1$ with then have $\deg r = 2$ and $\deg s = 1$ and $rq + sc = 0$.

Conversely suppose there exists non zero homogeneous polynomials r, s with degree 2 and 1 respectively such that $rq + sc = 0$, then we get that $rq = -sc$. Now note that $k[U,V]$ is a UFD we get that there exists some irreducible factor of q which divides c (because $\deg s < \deg q$, hence all the irreducible factors of q can not divide s). But then since k is algebraically closed the common irreducible factor has a root, hence q and c has a common root in $\mathbb{P}^1_k$.

Now it is evident that $rq+sc = 0$ for some non-zero homogeneous polynomials r, s of degree $2, 1$ respectively if and only if the polynomials u^2q, UVq, V^2q, Uc and Vc are linearly dependent. Thus q and c has a common root if there exists $x_0, \ldots, x_4 \in k$ (not all zero) such that

$$x_0U^2q + x_1UVq + x_2V^2q + x_3Uc + x_4Vc = 0. \tag{1}$$

Since homogeneous forms of degree 4, has a basis $\{U^4, U^3V, U^2V^2, UV^3, V^4\}$ writing in terms of this basis we get that equation (1) holds if and only if

$$\underbrace{\begin{bmatrix} a_0 & 0 & 0 & b_0 & 0 \\ a_1 & a_0 & 0 & b_1 & b_2 \\ a_2 & a_1 & a_0 & b_2 & b_3 \\ 0 & a_2 & a_1 & b_3 & b_2 \\ 0 & 0 & a_2 & 0 & b_3 \end{bmatrix}}_{\mathrm{res_{q,c}}} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Thus we get that they have a common root if and only if the matrix $\mathrm{res}_{q,c}$ is nonsingular, that is, the determinant $\det(\mathrm{res}_{q,c}) = 0$, which is equivalent to saying

$$\det \begin{vmatrix} a_0 & a_1 & a_2 & & \\ & a_0 & a_1 & a_2 & \\ & & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & \\ & b_0 & b_1 & b_2 & b_3 \end{vmatrix} = 0$$

Hence, proved.

Chapter 2

Problem 2.6. *Let $C : (y^2 = x^3 + x^2) \subset \mathbb{R}^2$. Show that a variable line through $(0,0)$ meets C at one further point, and hence deduce the parametrisation of C given in (2.1). Do the same for $(y^2 = x^3)$ and $(x^3 = y^3 - y^4)$.*

- We are given the curve $C : (y^2 = x^3 + x^2)$. Consider the variable line $y = \lambda x$. Plugging this in the equation defining C we get,
$$\lambda^2 x^2 = x^3 + x^2 \implies x^2(x + 1 - \lambda^2) = 0\,.$$
So, for $x \neq 0$ we get $x = \lambda^2 - 1$, and hence, $y = \lambda^3 - \lambda$. Therefore C is parametrised as $t \mapsto (t - 1, t^2 - t)$.

- We are given the curve $C : y^2 = x^3$. Consider the variable line $y = \lambda x$. Plugging this in the equation defining C we get,
$$\lambda^2 x^2 = x^3 \implies x^2(x - \lambda^2) = 0\,.$$
So, for $x \neq 0$ we get $x = \lambda^2$, and hence, $y = \lambda^3$. Therefore C is parametrised as $t \mapsto (t^2, t^3)$.

- We are given the curve $C : x^3 = y^3 - y^4$. Consider the variable line $x = \lambda y$. Plugging this in the equation defining C we get,
$$\lambda^3 y^3 = y^3 - y^4 \implies y^3(\lambda^3 - 1 + y) = 0\,.$$
So, for $y \neq 0$ we get $y = -\lambda^3 + 1$, and hence, $x = -\lambda^4 + \lambda$. Therefore C is parametrised as $t \mapsto (-t^4 + t, -t^3 + 1)$.

Problem 2.7. *Let $\varphi : \mathbb{R}^1 \to \mathbb{R}^2$ be the map given by $t \mapsto (t^2, t^3)$; prove directly that any polynomial $f \in \mathbb{R}[X, Y]$ vanishing on the image $C = \varphi(\mathbb{R}^1)$ is divisible by $Y^2 - X^3$. Determine what property of a field k will ensure that the result holds for $\varphi : k \to k^2$ given by the same formula. Do the same for $t \mapsto (t^2 - 1, t^3 - t)$.*

By the Euclidean algorithm for polynomials in Y, we get
$$f(X, Y) = a(X, Y)(Y^2 - X^3) + Y b(X) + c(X),$$
for some polynomials $a \in \mathbb{R}[X, Y]$, $b, c \in \mathbb{R}[X]$. Putting $X = t^2, Y = t^3$ we get,
$$0 = f(t^2, t^3) = t^3 b(t^2) + c(t^2).$$
But then, $t^3 b(t^2)$ contains only odd terms in t and $c(t^2)$ contains only even terms in t. Hence, $b = c = 0$ and so, $Y^2 - X^3 \mid f$ if f vanishes on $C = \{(t^2, t^3) \mid t \in \mathbb{R}\}$. ■

The property of the field k necessary for the above proof to go through is that k must be an infinite field.

Let f vanish on $\{(t^2 - 1, t^3 - 1) \mid t \in k\}$. We will show that f is divisible by $Y^2 - X^3 - X^2$ in $k[X, Y]$. By the Euclidean algorithm for polynomials in Y, we get
$$f(X, Y) = a(X, Y)(Y^2 - X^3 - X^2) + Y b(X) + c(X),$$
for some polynomials $a \in k[X, Y]$, $b, c \in k[X]$. Putting $X = t^2 - 1, Y = t^3 - 1$ we get,
$$0 = f(t^2 - 1, t^3 - 1) = (t^3 - t) b(t^2 - 1) + c(t^2 - 1).$$
Let $\deg b = k, \deg c = l$, so that $\deg(t^3 - t) b(t^2 - 1) = 2k + 3$ and $\deg c(t^2 - 1) = 2l$. Therefore, if their sum is 0 for all t, we must have $b = c = 0$.

Problem 2.8. *Let $C : (f = 0) \subset k^2$, and let $P = (a, b) \in C$; assume that $\frac{\partial f}{\partial x} \neq 0$. Prove that the line*
$$L : \left(\frac{\partial f}{\partial x} \cdot (x - a) + \frac{\partial f}{\partial y} \cdot (y - b) = 0 \right)$$
is the tangent line to C at P, that is, the unique line L of k^2 for which $f|_L$ has a multiple root at P.

Suppose ℓ is a line through $P = (a, b)$ such that $f|_\ell$ has a multiple root at P. Let ℓ be parametrised as $(x, y) = (a, b) + (\lambda, \mu)t$. Then, $f|_\ell(t) = f(a + \lambda t, b + \mu t)$. $P \in C$ means $f|_\ell(0) = f(P) = 0$ and the multiple root at P means $f|_\ell'(0) = 0$. But, by the chain rule,
$$f|_\ell'(0) = \lambda \frac{\partial f}{\partial x}\Big|_P + \mu \frac{\partial f}{\partial y}\Big|_P,$$
and so, $f|_\ell$ having a multiple root at P exactly means that $\ell \subseteq L$. As both these spaces are affine subspaces of dimension 1 through P, we get $\ell = L$, which proves the uniqueness of L. ■

Problem 2.9. *Let $C : (y^2 = x^3 + 4x)$, with the simplified group law (2.13). Show that the tangent line to C at $P = (2, 4)$ passes through (0,0), and deduce that P is a point of order 4 in the group law.*

Let $f = y^2 - x^3 + 4x$, so that $\frac{\partial f}{\partial x} = -16$, $\frac{\partial f}{\partial y} = 8$. Then, the tangent line to $C : (f = 0)$ is given by

$$\frac{\partial f}{\partial x}\Big|_P (x-2) + \frac{\partial f}{\partial y}\Big|_P (y-4) = 0 \implies y = 2x.$$

This line clearly passes through (0,0). Therefore, $P + P = \overline{(0,0)} = (0,0)$ using the group law on the cubic, and so $4P = (0,0) + (0,0) = \mathcal{O}$, the point at infinity. Hence, P is an element of order 4. ■

Problem 2.10. *Let $C : (y^2 = x^3 + ax + b) \subset \mathbb{R}^2$ be non-singular; find all points of order 2 in the group law, and understand what group they form. Now explain geometrically how you would set about finding all points of order 4 on C.*

In the simplified group law, (x, y) is an element of order 2 iff $\overline{(x, y)} = (x, -y)$ is equal to (x, y), i.e, $y = 0$ or $(x, y) = \mathcal{O}$ is the point at infinity. We now consider the following two cases.

- Suppose that $x^3 + ax + b = 0$ has a single real root α. Then, the cubic C has a single component which intersects the $y-$axis at $(\alpha, 0)$. Then the only point of order 2 is $(0, \alpha)$ and this forms the cyclic group on 2 elements with the identity $\mathcal{O}$, the point at infinity.
- Suppose that $x^3 + ax + b = 0$ has three real roots α, β, γ. Then the cubic C has two components which intersect the $y-$axis at $(\alpha, 0), (\beta, 0), (\gamma, 0)$. These three points are the only points of order 2 on C, and they form a group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with identity as $\mathcal{O}$.

If $P \in C$ is a point of order 4, it satisfies $4P = \mathcal{O}$, i.e, $2P$ is a point of order 2. With the previous results, we can find all such P geometrically by constructing the lines through the points where C intersects the $y-$axis and finding at which point (if any) where these lines are tangent to C.

Problem 2.11. *Let x, z be coordinates on k^2, and let $f \in k[x, z]$; write f as*

$$f = a + bx + cz + dx^2 + exz + fz^2 + \cdots .$$

Write down the conditions in terms of $a, b, c, \ldots$ that must hold in order that

- *$P = (0, 0) \in C : (f = 0)$*
- *the tangent line to C at P is $(z = 0)$*
- *P is an inflexion point of C with $(z = 0)$ as the tangent line.*

- $f(P) = 0 \implies a = 0$.
- The line $\ell : (z = 0)$ can be parametrised as $t \mapsto (t, 0)$, and so $f\big|_\ell(t) = a + bt + dt^2 + \cdots$. ℓ is a tangent at P iff $f\big|_\ell'(P) = 0$, i.e, $b = 0$.
- P is an inflexion point iff $f\big|_\ell''(P) = 0$, i.e, $d = 0$.

Problem 2.12. *Let $C \subset \mathbb{P}^2_k$ be a plane cubic, and suppose that $P \in C$ is an inflexion point; prove that a change of coordinates in $\mathbb{P}^2_k$ can be used to bring C into the normal form*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

We first fix coordinates so that $P = (0, 1, 0)$ and the tangent to C at P is given by $\ell : (z = 0)$. By Problem 6 above, we get that C is defined as the zero locus of a polynomial of the form $y^2z + yA(x, z) + B(x, z)$, where A, B are homogenous polynomials of degrees 2 and 3 respectively. We now find the vertical tangents of C apart from ℓ. The vertical line $x = \lambda z$ will be tangent to C iff λ is a root of the discriminant $-(A(\lambda, 1))^2 + 4B(\lambda, 1)$. Bezout's theorem tells us that any such line must have intersection multiplicity 2 with C, because $\deg C = 3$

and any vertical line must meet C at P. Therefore, there are 3 simple roots of the discriminant, and we get 3 distinct points P_1, P_2, P_3 on C at which the corresponding tangents meet C other than P.

We now claim that the points P_j are collinear. Let P' be the third point of intersection of $\overrightarrow{P_1P_2}$ and C. Consider the three cubics $C, \overrightarrow{PP_1}+\overrightarrow{PP_2}+\overrightarrow{PP'}, \ell+2\overrightarrow{P_1P_2}$. As these cubics intersect in the 8 points $3P, 2P_1, 2P_2, P'$, they must intersect at a ninth point by the Cayley-Bacharach theorem. This point must clearly be P', and so $\overrightarrow{PP'}$ intersects C twice at P', i.e, $P' = P_3$. By an appropriate change of coordinates, we can assume that $P_1 = (0,0,1), P_2 = (1,0,1)$ and $P_3 = (\alpha, 0, 1)$ for some α. These can be performed without affecting the coordinates of P and the line ℓ, and so all of the above remains valid. But now, $A(\lambda, 1)$ must vanish at $\lambda = 0, 1, \alpha$, which simply means that A is identically 0. Therefore, the equation of C becomes

$$y^2 z - x(x-z)(x-\alpha z) = 0,$$

which on expanding out the product is of the form to be shown. ■

Problem 2.13. *Consider the curve $C : (z = x^3) \subset k^2$; C is the image of the bijective map $\varphi : k \to C$ by $t \mapsto (t, t^3)$, so it inherits a group law from the additive group k. Prove that this is the unique group law on C such that $(0,0)$ is the neutral element and*

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear},$$

for $P, Q, R \in C$.

Throughout this solution, the notation $P(t)$ means $P = (t, t^3) \in C$. Suppose we give C the additive law induced from the abelian group structure of k, i.e, $P(t) + Q(s) = R(t+s)$. Then,

$$\begin{aligned} P(u) + Q(v) + R(w) &= 0 \\ \iff u + v + w &= 0 \\ \iff w^2 + u^2 + wu &= u^2 + v^2 + uv \\ \iff \frac{w^3 - u^3}{u^3 - v^3} &= \frac{w-u}{u-v} \end{aligned}$$

and the last equivalence simply means that $R(w)$ is collinear with $P(u), Q(v)$. Therefore, the group law inherited from k indeed satisfies the required condition.

Now suppose there is some law $*$ on C such that the required condition holds. We need to show that $P(t) + Q(s) = (t+s, (t+s)^3)$ for all $P, Q \in C$. Consider the point $R = (x, x^3)$ on C which is collinear with P, Q. Then,

$$\frac{x^3 - t^3}{t^3 - s^3} = \frac{x-t}{t-s} \implies (x-t)(x-s)(x+t+s) = 0,$$

and so, $R = (-t-s, (-t-s)^3)$. By the condition given we therefore get $(t, t^3) * (s, s^3) * (-t-s, (-t-s)^3) = (0,0)$. Putting $s = 0$, and using the fact that $(0,0)$ is the identity element, we get $\overline{P(t)} = (-t, -t^3)$. As $P+Q+R = (0,0)$ means that $R = \overline{(P+Q)}$, and we have shown that for $P(t), Q(s)$ we must have $R(-t-s)$, we get $P * Q$ is given by $(t+s, (t+s)^3)$. This is exactly the group law inherited from k, which proves the uniqueness. ■

Problem 2.14. *Prove that for $u, v \in \mathbb{Z}$,*

$$u^2 + v^2, u^2 - v^2 \text{ both squares} \implies v = 0.$$

Let $x, y \in \mathbb{Z}$ such that $u^2 + v^2 = x^2, u^2 - v^2 = y^2$, and assume $v \neq 0$. By dividing out any common divisors on both sides, we can assume without loss of generality that u, v, x, y are all pairwise coprime. Now, any odd square is congruent to 1 modulo 4, and any even square is 0 modulo 4. Therefore, as u, v have different parity, x^2 must be congruent to 1 mod 4, and so x is odd. If u is even and v is odd, we get $y^2 \equiv -1$ mod 4, which is not possible! So, u is odd, v is even and y is odd as well. Now consider the following factorisations:

$$\begin{aligned} (x-u)(x+u) &= v^2 \\ (u-y)(u+y) &= v^2 \\ (x-y)(x+y) &= 2v^2 \\ (2u - (x+y))(2u + (x+y)) &= 2(x^2+y^2) - (x+y)^2 = (x-y)^2. \end{aligned}$$

It is easily checked that as u, v, x, y are pairwise coprime and u, x, y are odd, v is even, the pairs of factors occurring on the LHS of each factorisation only share powers of 2 as common factors. Without loss of generality, we assume that $4 \nmid (x-y)$, replacing y by $-y$ if necessary.

Let $v = 2\widetilde{v}, x-u = 2a, x+u = 2b$ where a, b are coprime. Then, $4ab = 4\widetilde{v}^2 \implies ab = \widetilde{v}^2$. By the fundamental theorem of arithmetic, we get both a, b are squares and so, $x - u = 2v_1^2$ for some v_1. Similarly, we get $u - y = 2u_1^2$ for some u_1. If $x - y = 2c, x + y = 2d$ where $2 \nmid c$ and c, d are coprime, we get $cd = 2\widetilde{v}^2$. By assumption that $2 \nmid c$, we get $c, \frac{d}{2}$ are squares and so $x - y = 2x_1^2$ for some x_1. Finally, we also get $2u - (x + y) = 2y_1^2$ for some y_1. But then,

$$2u_1^2 + 2v_1^2 = u - y + x - u = x - y = 2x_1^2 \implies u_1^2 + v_1^2 = x_1^2$$
$$2u_1^2 - 2v_1^2 = u - y - x + u = 2u - (x + y) = 2y_1^2 \implies u_1^2 - v_1^2 = y_1^2.$$

Further, $|v_1| < \sqrt{x-u} \leq |v|$. Therefore, if we assume that (u, v) is a pair of coprime integers such that both $u^2 + v^2$ and $u^2 - v^2$ are squares, we arrive at a new pair (u_1, v_1) of coprime integers such that the same holds for this pair and $|v_1| < |v|$. By assumption $|v| \neq 0$, so we get an infinite set of pairs (u_j, v_j) such that $U - j^2 + v_j^2, u_j^2 - v_j^2$ are both squares and $|v_j| < |v_{j-1}|$. But this is impossible! Hence, by contradiction, we get $v = 0$. ■

Chapter 4

§ Problem 4.2

The polynomial map $\varphi : \mathbb{A}_k^1 \to \mathbb{A}_k^3$ is given by $X \mapsto (X, X^2, X^3)$. Let us call C be the image of φ. Let us consider the map

$$\varphi^* : k[X, Y, Z] \to k[T]$$

given by $X \to T, Y \to T^2, Z \to T^3$. We can see $(X^2 - Y, X^3 - Z)$ is contained in $\ker \varphi^*$, any elemenent $f \in k[X, Y, Z]$ can be written as, (using Eucledian algorithm twice)

$$f(x, y, z) = (x^3 - z)f_1(x, y, z) + (x^2 - z)f_2(x, y) + f_3(x)$$

If $f \in \ker \varphi^*$ then $f(T, T^2, T^3) = 0$ in other words $f_3(T) = 0$ for any T. So, any $f \in \ker \varphi^*$ is contained in $(X^3 - Z, X^2 - Y)$. It also proves that the ideal is a prime ideal, so $V(x^3 - z, x^3 - y)$ is irreducible. Thus we get, $C = V(x^3 - z, x^3 - y)$ and hence C is Algebraic set. Note that the co-ordinate rings for C is $K[C] = k[X, Y, Z]/I(V) \simeq k[X, Y, Z]/(X^2 - Y, X^3 - Z)$ and for $\mathbb{A}_k^1$ it is, $K[\mathbb{A}_k^1] = k[T]$. We have seen φ^* gives us the isomorphism between co-ordinate rings we can say the Algebraic set C and $\mathbb{A}_k^1$ are isomorphic. ■

§ Problem 4.4

If $\varphi : X \to Y$ is an isomorphism between X and a subvariety $\varphi(X) \subset Y$, then there is a isomorphism between the co-ordinate rings $k[X] \simeq k[\varphi(X)]$. Since, $\varphi(X) \subset Y$ we can say, $I(Y) \subset I(\varphi(X)) \subsetneq k[y_1, \cdots, y_n]$. This means we have a natural map

$$\pi : k[Y] \to k[\varphi(X)]$$

Any element in $k[\phi(X)]$ can be represented by $f + I(\varphi(X))$, where $f \notin I(\varphi(X))$, so $f \notin I(Y)$ and hence, $f + I(Y)$ will represent an element of $K[Y]$ which will maps to $f + I(\varphi(X))$ under π. Thus, we have a surjective map,

$$k[Y] \xrightarrow{\pi} k[\varphi(X)] \xrightarrow[\simeq]{\varphi^*} k[X]$$

It is not hard to note, $\varphi^* \circ \pi$ is the map $\Phi : K[Y] \to K[X]$.

For other direction suppose $\Phi : k[Y] \to k[X]$ is a surjective morphism. If $\ker \Phi = I$, it must be a prime ideal as $k[Y]/I \simeq k[X]$. The ring isomorphism induce isomorphism between variety X and subvariety $V(I) \subset Y$.

§ Problem 4.6

(i) Let, g be a rational map defined by $x \mapsto \frac{x-1}{x+1}$ and f is the map defined by $\frac{1-x}{1+x}$. The composition $g \circ f = \mathrm{id}$. So the map $g \circ f$ has domain $\mathbb{A}_k^1$ but domain of f is $\mathbb{A}_k^1 \setminus \{-1\}$. So domain of $g \circ f$ is larger than $\mathrm{dom}\ f \cap f^{-1}(\mathrm{dom}\ g)$.

(ii) Let C be any smooth curve through $(0,0)$. Then since C is smooth, if $C = V(g)$ for some $f \in \mathbb{R}[X,Y]$, it is not the case that $\frac{\partial g}{\partial x} = \frac{\partial f}{\partial y} = 0$ at $(0,0)$ (this is by the definition of smoothness). We may assume WLOG that $\frac{\partial f}{\partial y} \neq 0$ at $(0,0)$. Then by the implicit function theorem, in some small (analytic) neighbourhood U of $(0,0)$, $C = (x, h(x))$ for some $h : U \to \mathbb{R}$. h is smooth since C is. Then when $xy/\left(x^2+y^2\right)$ is restricted to C, in the neighbourhood U,

$$\frac{xy}{x^2+y^2} = \frac{xh(x)}{x^2+(h(x))^2}$$

which is smooth as $h(x)$ is. On the other hand $xy/\left(x^2+y^2\right)$ is not continuous in $\mathbb{R}^2$ as if it was, then its limit as we approached $(0,0)$ on the line $x=0$ and the line $x=y$ would be the same, but

$$\lim_{t\to 0} \frac{0\cdot t}{0^2+t^2} = 0 \neq \frac{1}{2} = \lim_{t\to 0} \frac{t^2}{t^2+t^2}$$

§ Problem 4.7

Let, $\varphi : \mathbb{A}_k^1 \to C$ is the parametrization $t \mapsto (t^2-1, t(t^2-1))$. If φ was parametrization then the following map $\Phi : k[x,y] \to k[t]$ by $x \mapsto (t^2-1), y \mapsto t(t^2-1)$ should have induced isomorphic between $k[C] = k[x,y]/(y^2 - x^2(x+1))$ and $k[\mathbb{A}_k^1] = k[t]$. But we know by isomorphism theorem, $k[x,y]/(y^2-x^2(x+1)) = \mathrm{Im}(\Phi) = k[t^2-1, t(t^2-1)]$. We can show this is not the full $k[t]$ as t is not in the above ideal. Otherwise,

$$t = g(-,-)(t^2-1) + f(-,-)(t^3-t^2)$$

would give us $1=0$, which is not possible. So, φ is not an isomorphism.

The restriction $\varphi' : \mathbb{A}_k^1 \setminus \{1\} \to C$ is an isomorphism. As the inverse image of $(0,0)$ under the restriction map is one point -1 and at other points it is bijection. The map $\psi : C \setminus (0,0) \to \mathbb{A}_k^1$, given by $(x,y) \mapsto y/x$ will help us to say $\varphi : \mathbb{A}_k^1 \setminus \{\pm 1\} \to C \setminus \{(0,0)\}$ is an isomorphism. And thus, it is a bijection. So the map, φ' we are given is also a bijection (isomorphism).

§ Problem 4.8

The given problem does not make any sense ! We perhaps try to make the question correct by assuming $\psi : C \to \mathbb{A}_k^1$ is $(x,y) \mapsto y/x$. It's not hard to see this function is in $k(C)$. So it a rational function. Let, $\varphi : \mathbb{A}_k^1 \to C$ be the parametrization $t \mapsto (t^3-1, t(t^3-1))$. We can see $\psi \circ \varphi = \mathrm{id}$. The function y/x is not defined at $x=0$. On the curve $x = 0 \implies y = 0$. The inverse image of $(0,0)$ under the map φ is three points in k satisfying $t^3 - 1 = 0$ (assuming k to be algebraically closed). So the restriction of φ gives us isomorphism between

$$\mathbb{A}_k \setminus \{3 \text{ points}\} \to C \setminus \{(0,0)\}$$

§ Problem 4.9

Just by degree analysis we can conclude $(xt - yz)$ is irreducible and hence the ideal is prime. $k[V]$ is given by $k[x,y,z,t]/(xt-yz)$. We will show, x,y,z,t are irreducible thus $xt = yz$ in the ring $k[V]$ means it can't be UFD. If x as not irreducible then we could write $x = fg$ now by degree analysis we can see one of f,g must have degree 0, degree 0 elements are unit. So, x is irreducible and our proof is complete. ■

Second part of this question deos not make sense as $y=0$ can't be contained in $\mathrm{dom}\, f$.

§ 4.11

(i) (i) If $V = V(\{f_i\} i \in I)$, and $W = V(\{g_j\} j \in J)$ for some I, J where $f_i \in k[X_1, \ldots, X_n]$, and $g_j \in k[X_1, \ldots, X_m]$. Then $V \times W = V\left(\{\bar{f}i\} i \in I \cup \{\bar{g}j\} j \in J\right)$ where $\bar{f}i$ is the image of f_i under the morphism $k[X_1, \ldots, X_n] \to k[X_1, \ldots, Xn+m]$ that sends X_k to X_k, and $\bar{g}j$ is the image of g_j under the morphism $k[X_1, \ldots, X_m] \to k[X_1, \ldots, Xn+m]$ that sends X_k to X_{n+k}.

(ii) Let $V = W = A^1$. By the definition of product topologies and the definition of open sets in A^1, the only open sets in $A^1 \times A^1$ with the product topology are the entire space minus finitely many horizontal and vertical lines. But the zero locus of $X^2 + Y^2 - 1$ is closed in $A^1 \times A^1$ with the Zariski topology (by its definition), and its complement is not the entire space minus finitely many horizontal and vertical lines.

(iii) Suppose that $V \times W$ was reducible. Then $V \times W = X_1 \cup X_2$ for some closed disjoint nonempty X_1, X_2 in A^{n+m}. Let $V_i = \{v \in A^n \mid \{v\} \times W \subset X_i\}$. Observe that $V_1 \amalg V_2 = V$. For clearly V_1, V_2 are disjoint since X_1, X_2 are disjoint. Moreover, for all $v \in V$, if $\{v\} \times W$ was contained in neither X_1 nor X_2, the pullbacks of $X_1 \cap \{v\} \times W$ and $X_2 \cap \{v\} \times W$ along the inclusion $W \to V \times W$ (which is a continuous map) would show that W wasn't irreducible, contradiction. Finally, V_1, V_2 are closed since they are the intersections of the sets of the form $V_{1w} = \{v \in A^n \mid \{v\} \times \{w\} \subset X_1\}$ and $V_{2w} = \{v \in A^n \mid \{v\} \times \{w\} \subset X_2\}$ for all $y \in W$, but since those sets are the fibers of either point sets or the empty set in A^{n+m} under the inclusion $V \to V \times W$, and arbitrary intersections of closed sets are closed, the result follows.

(iv) If $f : V \to V'$ and $g : W \to W'$ are isomorphisms, with the inverses $f^{-1}, g^{-1}, f \times g : V \times W \to V' \times W'$ is an isomorphism with the inverse $f^{-1} \times g^{-1}$.

§ 4.12

(a) Let $f \in k(X, Y)$ be a rational function not regular at $(0, 0)$. Since $k[X, Y]$ is a UFD, $f = u/v$ for some $u, v \in k[X, Y]$ with no common factors. Then if $v(0, 0) = 0, v$ would not be a constant, so by exercise 3.13 (b) $V(v)$ would be infinite, and f would not be regular at the points on the curve defined by the zero set of v.

(b) Suppose for the sake of contradiction that $\mathbb{A}_k^2 \backslash \{(0, 0)\}$ is affine. The co-ordinate ring of $\mathbb{A}_k^2 \backslash \{(0, 0)\}$ is precisely the subring of functions $f \in k\left(\mathbb{A}_k^2\right)$ that are regular everywhere except $(0, 0)$. But by part (a), any such function must be regular at $(0, 0)$ too. So the co-ordinate ring of $\mathbb{A}_k^2 \backslash \{(0, 0)\}$ is just the ring of regular functions on $\mathbb{A}_k^2$, i.e. $k[X, Y]$. So the inclusion $\mathbb{A}_k^2 \backslash \{(0, 0)\} \hookrightarrow \mathbb{A}_k^2$ would induce a map from $k[X, Y]$ to the

Ring of regular functions on $\mathbb{A}_k^2 \backslash \{(0, 0)\}$ that is surjective since the latter ring is just $k[X, Y]$, and injective as if $f \in k[X, Y]$ is 0 on $\mathbb{A}_k^2 \backslash \{(0, 0)\}$, $f = 0$. So the induced map would be a ring isomorphism, so the inclusion $\mathbb{A}_k^2 \backslash \{(0, 0)\} \hookrightarrow \mathbb{A}_k^2$ would have to be an isomorphism between varieties too, but it is not surjective. Contradiction.