Set # 1: Revisiting old friends

Terminology

T1. What is a ring? What is a field? Give some examples of fields and of rings that are not fields.

T2. What is a homomorphism between two rings? What is an isomorphism between two rings?

T3. What is the Legendre symbol $\left(\frac{a}{p}\right)$?

Exploration

E1. Consider the following number systems (rings): $\mathbb{Z}$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{2}]$. Which of these has a division algorithm? Which is a unique factorization domain? What are the units in each?

E2. Remind yourself of the following result (Set #19 P2): for every prime p, the equation $x^2 + y^2 + 1 = 0$ has a solution in $\mathbb{Z}/p$. Can you determine the exact number of solutions?

Numerical Problems (some food for thought)

N1. Find all integer solutions to $71x + 32y = 1$. Find all solutions in $\mathbb{Z}/5[x]$ to $(x^2 + x + 1)p(x) + (x^4 + 1)q(x) = 1$. Find all solutions in $\mathbb{Z}[i]$ to $17\alpha + (2 + 5i)\beta = 1$.

N2. For which primes p is the equation $x^2 \equiv 11 \pmod{p}$ solvable in $\mathbb{Z}/p$?

N3. Which of the following rings are fields? $\mathbb{Z}[i]/3$. $\mathbb{Z}[\sqrt{-2}]/3$. $\mathbb{Z}/3[x]/(x^2+x+1)$. $\mathbb{Z}/3[x]/(x^2+1)$. Which if any of these rings are isomorphic to each other?

Prove or Disprove and Salvage if Possible

P1. Let F be a field with finitely many elements. Show that there is a unique prime number p such that $p = 0$ in F.

P2. Show that any homomorphism between fields is injective.

P3. Let F be a finite field with q elements. Show that q is a power p^r of some prime number p, and that every element $a \in F$ satisfies $a^q = a$. In fact, F is a field containing $\mathbb{F}_p$ in which the polynomial $x^q - x \in \mathbb{F}_p[x]$ factors into a product of linear factors; and F contains no smaller subfield where this property holds. (F is then known as a "splitting field" of the polynomial $x^q - x$.)

Set #2

Terminology

T1. What is an algebraic number? What is an algebraic integer? We will write $\overline{\mathbb{Z}}$ and $\overline{\mathbb{Q}}$ for the sets of all algebraic integers and algebraic numbers, respectively.

T2. Let F be a field. What is a vector space over F? What is a basis of a vector space over F?

Exploration

E1. Recall Set #13 A2, which asked you to classify rational solutions to $x^2 + y^2 = 1$ (and thereby classify integer Pythagorean triples) using a geometric method: that is, to start with a single solution (eg, $(0, 1)$), and then to draw chords of rational slope through this point and calculate their second point of intersection with the circle. Do this if you have not done so already! Can you use a version of this argument to give an illuminating solution to Set #1 E2? What other equations would this method apply to?

E2. Let γ_1, γ_2 be non-zero complex numbers, and consider their integer linear combinations $M = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$ and their rational linear combinations $V = \mathbb{Q}\gamma_1 + \mathbb{Q}\gamma_2$ (both M and V are subsets of the complex numbers). Let α be any complex number, and assume that $\alpha \cdot V = \{\alpha v : v \in V\}$ is contained in V. Show that α satisfies a quadratic equation with rational coefficients, so in particular α is an algebraic number. If moreover $\alpha \cdot M \subset M$, show that α is an algebraic integer. Can you generalize your reasoning to the analogous situation where M and V are now generated by some finite collection $\gamma_1, \ldots, \gamma_r$ of non-zero complex numbers?

Numerical Problems (some food for thought)

N1. Determine all algebraic integers inside the following fields: $\mathbb{Q}$; $\mathbb{Q}[i]$; $\mathbb{Q}[\sqrt{-3}]$; $\mathbb{Q}[\sqrt{2}]$.

N2. Show that $\sqrt[3]{2}$ and $\sqrt{5}$ are algebraic integers. Show that their sum $\sqrt[3]{2} + \sqrt{5}$ and their product $\sqrt[3]{2} \cdot \sqrt{5}$ are also algebraic integers. Might the sum and product of two algebraic integers always be algebraic integers?

Prove or Disprove and Salvage if Possible

P1. Let V be a finite-dimensional vector space over a field F. Show that V has a basis. Use this to give another proof that any finite field has p^r elements for some prime p and positive integer r.

P2. Any algebraic number α is the root of a unique monic irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Moreover, if $g(x) \in \mathbb{Q}[x]$ is any polynomial for which $g(\alpha) = 0$, then $f(x)$ divides $g(x)$ (in $\mathbb{Q}[x]$).

Set # 3

Terminology

(1) What is the Möbius function $\mu(n)$?
(2) What is the Euler φ function $\varphi(n)$?

Exploration

E1. For every prime p, construct a finite field with p^2 elements. Do you have more than one way of making such a field? Are the results isomorphic?

E2. Let $f\colon \mathbb{N} \to \mathbb{C}$ be any function defined on the positive integers $\mathbb{N}$. Define a new function $g\colon \mathbb{N} \to \mathbb{C}$ by $g(n) = \sum_{d|n} f(d)$. Express $f(1), f(2), \ldots, f(12)$ in terms of values of g. What patterns do you notice? Any conjectures?

Numerical Problems (some food for thought)

N1. Consider a *conic* $V = \{(x, y) : ax^2 + bxy + cy^2 + dx + ey + f = 0\}$ with coefficients $a, b, \ldots, f$ in the finite field $\mathbb{F}_p$. Suppose that V has a solution (x_0, y_0) with $x_0, y_0 \in \mathbb{F}_p$. How many solutions in $\mathbb{F}_p$ does V then have?

N2. Which conics (as in N1) over $\mathbb{F}_2$ have *no* point over $\mathbb{F}_2$?

N3. Factor the following polynomials in the ring $\mathbb{F}_3[x]$: $x^3 - x$, $x^9 - x$, $x^{27} - x$. What do you notice?

N4. Repeat N2, but now factor the given polynomials in the ring $\mathbb{F}_9[x]$, where $\mathbb{F}_9$ is a field with 9 elements as in E1.

Prove or Disprove and Salvage if Possible

P1. $\overline{\mathbb{Z}}$ is a ring. $\overline{\mathbb{Q}}$ is a field. (Hint: Use Set #2 E2.)

P2. Consider the simple case of a conic V of the form $ax^2 + by^2 + c = 0$, where $a, b, c \in \mathbb{F}_p$ are all non-zero. Then $V(\mathbb{F}_p)$ is non-empty. What happens when some of a, b, c are zero?

P3. Let F be any field, and let $p(x) \in F[x]$ be an irreducible polynomial. Then $K = F[x]/p(x)$ is a field containing F, and there is an element $\alpha \in K$ such that $p(\alpha) = 0$. Moreover, K is equal to the set of linear combinations $F + F\alpha + F\alpha^2 + \cdots + F\alpha^{d-1}$, where d is the degree of $p(x)$, and the dimension of K as an F-vector space is d.

Set #4

Terminology

T1. What is a root of unity?

T2. Given three algebraic integers $\alpha, \beta, \gamma \in \overline{\mathbb{Z}}$, what does it mean to say $\alpha \equiv \beta \pmod{\gamma}$? If α, β, γ are in fact ordinary integers, is this notion consistent with our usual notion of congruence in $\mathbb{Z}$?

Exploration

E1. Consider the following two examples of the situation studied in Set #3 E2, in which we take f to be (i) the Euler φ function; (ii) the function $\psi(n)$ that records the number of elements of exact order n in some fixed field F. What comparison can you make between the functions φ and ψ, in light of Set # 12, E1?

E2. Let R be any ring, and let $f(x) = \sum_{i \geq 0} a_i x^i \in R[x]$ (implicitly $a_i = 0$ for all i greater than some integer d, the degree of f) be a polynomial with coefficients in R. Then we can define the "derivative" of f by the formula $f'(x) = \sum_{i \geq 1} i a_i x^{i-1} \in R[x]$. When R is the real numbers, this agrees with the construction in calculus, but it is a purely algebraic definition that makes sense in rings where the usual operations of calculus would not make sense, such as $R = \mathbb{F}_p$. Which of the familiar differentiation rules from calculus (eg, the product rule) continue to hold in this setting? Do antiderivatives exist?

Numerical Problems (some food for thought)

N1. Check that $\mathbb{F}_{17}^{\times}$ is cyclic. How many generators does it have? Check that $(\mathbb{Z}[i]/3)^{\times}$ is cyclic. How many generators does it have?

N2. In this problem, work over a field F of characteristic not 2. When we "complete the square" to solve a quadratic equation $x^2 + bx + c = 0$, we are defining a new variable $w = x + \frac{b}{2}$ and reducing to solving the simpler equation $w^2 + c - \frac{b^2}{4} = 0$. Starting with the equation $x^2 + 6xy + y^2 + 3x + 2y + 7 = 0$, perform a similar "change of variables" to produce a new equation of the form $aw^2 + bz^2 + c = 0$ (here w and z are the new variables) whose solutions (w, z) are in bijection with solutions (x, y) of the original equation via your change of variables. Do the same for the equation $xy + x + y = 0$. How general is this method?

Prove or Disprove and Salvage if Possible

P1. Let $f\colon \mathbb{N} \to \mathbb{C}$ be an arithmetic function, and let g be defined by $g(n) = \sum_{d|n} f(d)$. Then $f(n) = \sum_{d|n} g(d)\mu(\frac{n}{d})$.

P2. The multiplicative group of a finite field is cyclic. Can you make an analogous statement for general fields?

P3. Let F be a finite field of characteristic p. Then there is an element $\alpha \in F$ such that $F = \mathbb{F}_p[\alpha]$.

P4. If $\alpha, \beta \in \overline{\mathbb{Z}}$ and p is prime, then $(\alpha + \beta)^p \equiv \alpha^p + \beta^p \pmod{p}$ (congruence in $\overline{\mathbb{Z}}$ as in T2).

Set # 5

Terminology

T1. Let K be a field containing another field F. What do we mean by the degree of the field extension K/F?

Exploration

E1. The arithmetic of roots of unity is very closely related to quadratic reciprocity; this exercise is a first step in this direction. Let $\zeta = e^{2\pi i/8}$. Check that $(\zeta + \zeta^{-1})^2 = 2$, hence that $(\zeta + \zeta^{-1})^{p-1} = 2^{\frac{p-1}{2}}$. Use this and Set #4 P4 to give a new proof that $\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 8; \\ -1 \text{ if } p \equiv \pm 3 \pmod 8 \end{cases}$.

E2. Let F be any field. Under what conditions on integers d and n does the polynomial $x^d - 1$ divide the polynomial $x^n - 1$ in $F[x]$?

Numerical Problems (some food for thought)

N1. The subset $\mathbb{Q}[\sqrt[3]{2}] = \{\sum_{i=0}^{n} a_i \sqrt[3]{2}^i \mid n \in \mathbb{Z}, a_i \in \mathbb{Q}\}$ of $\mathbb{C}$ is a field.

N2. Let x_0 be either solution to $x_0^2 \equiv 2 \pmod 7$ (so $x_0 \equiv \pm 3 \pmod 7$). Show that for every integer n there is a solution $x_n^2 \equiv 2 \pmod{7^{n+1}}$ with $x_n \equiv x_0 \pmod 7$.

Prove or Disprove and Salvage if Possible

P1. Let F be a field, and let $f(x) \in F[x]$ be any polynomial. There is a field K containing F in which $f(x)$ factors as a product of linear factors $f(x) = \prod_i (x - \alpha_i)$, and the roots α_i are all distinct if and only if $f(x)$ and $f'(x)$ are coprime in $F[x]$. (K is called a "splitting field" of the polynomial F.)

P2. In $\mathbb{F}_p[x]$, the polynomial $x^{p^n} - x$ factors as the product of all irreducible monic polynomials in $\mathbb{F}_p[x]$ of degree dividing n.

P3. For all primes p and all positive integers n, there is a field with p^n elements. (The problems encountered so far suggest two proofs of this result!)

P4. Consider a conic $f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$ over a field F. Assume that the polynomial $f(x, y)$ is irreducible (in the polynomial ring $F[x, y]$) and moreover remains irreducible in $K[x, y]$ for any finite extension K/F (so for instance, $x^2 + y^2$ is irreducible in $\mathbb{R}[x, y]$ but reducible in $\mathbb{C}[x, y]$ since it equals $(x + iy)(x - iy)$). Show that there is a field extension K/F (of finite degree) such that after a suitable ("affine") change of variables V becomes equivalent either to the conic $z = w^2$ or to the conic $wz = 1$. Give an example where the field extension K/F is necessary to realize this equivalence. If $F = \mathbb{F}_2$, is it necessary?

Set # 6

Terminology

T1. What is a character $\chi\colon G \to \mathbb{C}^\times$ of a group G? What is the trivial character $\mathbb{1}$ of G?

T2. Let $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character of the group $\mathbb{F}_p^\times$, and let $a \in \mathbb{F}_p$. What is the Gauss sum $G_a(\chi)$? When $a = 1$, we will often write simply $G(\chi)$.

Exploration

E1. Let $\chi(t) = \left(\frac{t}{p}\right)$ be the Legendre symbol. Compute the Gauss sums $G(\chi)$ for $p = 3, 5, 7, 11, 13$. What do you notice? Any conjectures? Might this help us, as in Set #5 E1, gain new insight into quadratic reciprocity?

Numerical Problems (some food for thought)

N1. Solve the equation $x^3 + x + 1 \equiv 0 \pmod{11^3}$. Show that for all n, $x^3 + x + 1 \equiv 0 \pmod{11^n}$ has solutions. How many are there?

N2. Does the method of N1 (and Set #5 N2) apply to solving the congruences $x^2 + x + 1 \equiv 0 \pmod{3^n}$?

N3. Give an example of a character of the *additive* group $\mathbb{F}_p$; that is, produce a function $\psi\colon \mathbb{F}_p \to \mathbb{C}^\times$ such that $\psi(a + b) = \psi(a)\psi(b)$. Can you classify all such ψ?

Prove or Disprove and Salvage if Possible

P1. If χ is a character of a finite group G, then $\sum_{g\in G} \chi(g) = \begin{cases} 0 \text{ if } \chi \neq \mathbb{1}; \\ |G| \text{ if } \chi = \mathbb{1}. \end{cases}$

P2. Let G be any group. Then the set of all characters of G is an abelian group under the composition law $(\chi_1 \cdot \chi_2)(g) = \chi_1(g)\chi_2(g)$.

P3. If χ is a character of $\mathbb{F}_p^\times$ and $a \in \mathbb{F}_p$, then $G_a(\chi) = \chi(a^{-1})G_1(\chi)$.

P4. Let F be a field, and let $p(x) \in F[x]$ be a polynomial. Let K_1 and K_2 be any two splitting fields of $p(x)$. Then K_1 and K_2 are isomorphic.

Set # 7

Terminology

T1. What is the n-dimensional affine space over a field?

T2. What is the n-dimensional projective space over a field?

Exploration

E1. We have already made a thorough study of the equation $x^2 + y^2 + 1 = 0$, describing its solutions in the affine space $\mathbb{A}^2(\mathbb{F}_p)$. Recall that the number of solutions depended on the congruence class $p \pmod 4$. What happens if we consider the corresponding *projective* equation $X^2 + Y^2 = Z^2$, to be solved in $\mathbb{P}^2(\mathbb{F}_p)$. How doe the number of solutions depend on p? Can you generalize your observations to the study of other (non-degenerate?) conics in $\mathbb{P}^2$?

E2. Consider a general conic in projective space $V = \{[X, Y, Z] \in \mathbb{P}^2 : aX^2 + bXY + cY^2 + dXZ + eYZ + fZ^2 = 0\}$ over the finite field $\mathbb{F}_p$. Is $V(\mathbb{F}_p)$ always non-empty?

Numerical Problems (some food for thought)

N1. How many elements are there in $\mathbb{P}^n(\mathbb{F}_q)$? (Here as usual $\mathbb{F}_q$ is a finite field with q elements.)

N2. Let ζ be a primitive p^{th} root of unity. For any $a \in \mathbb{F}_p$, evaluate the sum $\sum_{t \in \mathbb{F}_p} \zeta^{at}$.

Prove or Disprove and Salvage if Possible

P1. Let $\mathbb{F}_q$ be a finite field with q elements. Then the *group* of characters of $\mathbb{F}_q^\times$ is cyclic of order $q - 1$.

P2. Let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be the Legendre symbol. Then $G(\chi)^2 = (-1)^{\frac{p-1}{2}} p$ (p an odd prime). (Hint: Evaluate the sum $\sum_{a \in \mathbb{F}_p} G_a(\chi) G_{-a}(\chi)$ in two ways.)

P3. Use P2 and the method of Set #5 E1 to give a new proof of quadratic reciprocity!

P4. For every prime p and positive integer n, there is a field with p^n elements, and any two fields with p^n elements are isomorphic.

Set #8

Terminology

T1. What is Newton's method?

T2. What is a line in the projective space $\mathbb{P}^2_F$ over a field F?

Exploration

E1. If p is an odd prime, then the number of solutions to $x^2 = a \pmod p$ is $1+\left(\frac{a}{p}\right)$. A seemingly naïve way to count solutions over $\mathbb{F}_p$ to $x^2 + y^2 = 1$ (or similar equations) is to compute

$$\sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} (1 + \left(\frac{a}{p}\right))(1 + \left(\frac{b}{p}\right)).$$

Expand the product and evaluate each of the four resulting sums to compute $N_p(x^2+y^2 = 1)$. Does the same approach work for $N_p(x^2 + y^2 = -1)$? How would you begin to generalize this method to count $N_p(x^n + y^n = 1)$?

Numerical Problems (some food for thought)

N1. Can you solve the equation $x^2 \equiv 17 \pmod{2^n}$ for all positive integers n? For which integers a can $x^2 \equiv a \pmod{2^n}$ be solved for all n?

N2. Let F be a field, and consider two lines L_1 and L_2 in affine space $\mathbb{A}^2_F$. In how many points do L_1 and L_2 intersect? What if we replace L_1 and L_2 by lines in the projective space $\mathbb{P}^2_F$?

N3. Consider conic sections as you meet them in high school algebra class, i.e. the set of *real* solutions to a degree 2 polynomial $f(x, y) \in \mathbb{R}[x, y]$. For two such real conics f and g, what is the possible number of points of intersection of $\{f = 0\}$ and $\{g = 0\}$ inside $\mathbb{A}^2(\mathbb{R})$?

N4. Let n be a positive integer. For $F = \mathbb{F}_p, \mathbb{Q}, \mathbb{C}$, how many more solutions does the projective equation $X^n + Y^n = Z^n$ have in $\mathbb{P}^2(F)$ than the affine equation $x^n + y^n = 1$ has in $\mathbb{A}^2(F)$?

Prove or Disprove and Salvage if Possible

P1. Let $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}^\times$ be any non-trivial character. Then $|G(\chi)| = \sqrt{p}$.

P2. Let F be a field, and let $f(x) \in F[x]$ be a polynomial of degree d. Then for any $a \in F$, we have the polynomial identity

$$f(x) = \sum_{k=0}^{d} \frac{f^{(k)}(a)}{k!}(x - a)^k.$$

P3. Let $f(x) \in \mathbb{Z}[x]$, and suppose there is an integer x_0 such that $f(x_0) \equiv 0 \pmod p$. If moreover $f'(x_0) \not\equiv 0 \pmod p$, then for all $n \geq 1$ there is an $x_n \in \mathbb{Z}$ such that $f(x_n) \equiv 0 \pmod{p^{n+1}}$. Additionally, if we require $x_n \equiv x_0 \pmod p$, then x_n is unique modulo p^{n+1}; and we may take $x_{n+1} \equiv x_n \pmod{p^{n+1}}$. Explain the analogy with Newton's method.

Set #9

Terminology

T1. For characters $\chi_1, \chi_2 \colon \mathbb{F}_p^\times \to \mathbb{C}^\times$, what is the Jacobi sum $J(\chi_1, \chi_2)$?

T2. What is a metric? What is the absolute value associated to a metric (and vice-versa)? What is the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$?

Exploration

E1. We have set down axioms for the integers on which we have based all of our work. The construction of the rational numbers from the integers is straightforward: $\mathbb{Q}$ is the "field of fractions" of $\mathbb{Z}$. How can we rigorously construct the real numbers starting from the rational numbers? Consider the following: there are sequences of rational numbers (for instance, the successive steps in the decimal approximation to $\sqrt{2}$ that do not have a *limit* in $\mathbb{Q}$. We can construct the real numbers, informally speaking, as a set of limits of sequences in $\mathbb{Q}$ in which the terms are getting arbitrarily close together. More precisely, $\mathbb{R}$ is the set of *Cauchy sequences* $(x_1, x_2, \ldots)$ of rational numbers (in the standard archimedean metric!), modulo the *equivalence relation* $(x_1, x_2, \ldots) \sim (y_1, y_2, \ldots) \iff \lim_{n\to\infty} |x_n - y_n| = 0$. Show that with these definitions, $\mathbb{R}$ inherits (a) binary operations + and $\cdot$ making it into a field containing $\mathbb{Q}$ as a subfield; and (b) an absolute value $|\cdot|$ extending the standard absolute value on $\mathbb{Q}$.

E2. Consider the projective conic $V = \{X^2 + Y^2 = Z^2\} \subset \mathbb{P}^2$ over a field F of characteristic not equal to 2. Fix an F-rational point: for definiteness, let us take the point $O = [1, 0, 1]$. Define a binary operation $\oplus$ on $V(F)$ as follows: for $P, Q \in V(F)$, there is a unique line L through O parallel to the line joining P and Q, and we let $P \oplus Q$ be the second point of intersection of V with L. Show that this procedure gives a well-defined binary operation on $V(F)$. Does $\oplus$ define a commutative group law on $V(F)$?

Numerical Problems (some food for thought)

N1. Evaluate: $|13|_5$; $|25|_5$; $|\frac{7}{5}|_5$; $|100!|_5$.

N2. Evaluate: $J(\mathbb{1}, \mathbb{1})$; $J(\mathbb{1}, \chi)$ for any non-trivial χ; $J(\chi, \chi^{-1})$ for any non-trivial χ. What does the last calculation have to do with Set #8 E1?

N3. Let F be a field. Consider the conics $C_1 = \{x^2 + y^2 = 1\}$ and $C_2 = \{y = x^2\}$ inside $\mathbb{A}^2(F)$. How does the number of points of intersection $\#(C_1 \cap C_2)(F)$ depend on F? What is the maximal number of points of intersection? For any field F, is there a finite extension K/F such that $\#(C_1 \cap C_2)(K)$ achieves this maximal number?

N4. The line $x = 1$ intersect the parabola $y = x^2$ in $\mathbb{A}^2(\mathbb{C})$ in one point. If we take the projective closures of these curves, in how many points do they intersect in $\mathbb{P}^2$? Which lines in $\mathbb{A}^2$ have the property that they intersect $y = x^2$ in an "extra point" when the intersection is taken in $\mathbb{P}^2$ instead of $\mathbb{A}^2$?

Prove or Disprove and Salvage if Possible

P1. Show that $|\cdot|_p$ is an absolute value on $\mathbb{Q}$; show that it satisfies the following strong form of the triangle inequality: $|a + b|_p \leq \max(|a|_p, |b|_p)$.

P2. Let $\chi_1, \chi_2 \colon \mathbb{F}_p^\times \to \mathbb{C}^\times$ be non-trivial characters such that $\chi_1\chi_2$ is also non-trivial. Then

$$J(\chi_1, \chi_2) = \frac{G(\chi_1)G(\chi_2)}{G(\chi_1\chi_2)}.$$

In particular, $|J(\chi_1, \chi_2)| = \sqrt{p}$. (Problem set continues on back)

P3. Use P2 (!) to give another proof that every prime $p \equiv 1 \pmod 4$ is a sum of two integer squares.

Set # 10

Terminology

T1. What are the p-adic integers $\mathbb{Z}_p$? What are the p-adic numbers $\mathbb{Q}_p$?

T2. What does it mean for a curve in the (affine or projective) plane to be non-singular?

T3. What is meant by the degree of a polynomial in two (or more) variables? What is a homogeneous polynomial?

Exploration

E1. Does your construction of the real numbers from Set #9 E1 generalize to let you construct a new number system from $\mathbb{Q}$ by working with the p-adic absolute value $|\cdot|_p$ (or indeed any absolute value?) rather than with the archimedean absolute value? Is the resulting "completion" a field? Does it contain an element we might fairly represent as $\sum_{i=0}^{\infty} p^i$?

E2. Consider the cubic equation $y^2 = x^3 + x + 1$. Count the number of solutions to this equation in $\mathbb{F}_p$ for $p = 2, 3, \ldots, 13$. Do you notice a pattern analogous to what you found in Set #3 N1?

E3. Let $F(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ be a homogeneous polynomial of degree m, and let $G(X, Y, Z)$ be a linear homogeneous polynomial, so that $\{F = 0\}$ and $\{G = 0\}$ are, respectively, a degree m curve and a line in $\mathbb{P}^2(\mathbb{C})$. What are the possibilities for the number of points of intersection of the projective curves $\{F = 0\}$ and $\{G = 0\}$ in $\mathbb{P}^2(\mathbb{C})$? Is there a "typical" number of points of intersection? What is happening when this "typical" number is not achieved?

Numerical Problems (some food for thought)

N1. Find an integer polynomial $f(x) \in \mathbb{Z}[x]$ and a prime p such that the equation $f(x) \equiv 0 \pmod{p^{10}}$ has a solution, but for which there exists n such that $f(x) \equiv 0 \pmod{p^n}$ does not have a solution.

N2. Find all primes p for which the equation $x^2 + 3 = 0$ has a solution in $\mathbb{Z}_p$. Do the same for $x^2 + 1 = 0$.

N3. For which primes p does $x^2 + y^2 + 1 = 0$ have a solution in $\mathbb{Q}_p$? What about $x^2 + 7y^2 = 1$?

N4. Over which fields F is the affine curve $x^5 + y^5 = 1$ non-singular? What about the affine curve $y^2 = x^3 + 35$?

Prove or Disprove and Salvage if Possible

P1. We have defined $\mathbb{Z}_p$ as the set of sequences $(a_n)_n \in \prod_{n\geq 1} \mathbb{Z}/p^n$ such that $a_{n+1} \equiv a_n \pmod{p^n}$. How do we define addition and multiplication on $\mathbb{Z}_p$? Show that with these definitions $\mathbb{Z}_p$ is a ring, and $\mathbb{Q}_p$ is a field.

P2. If $a \in \mathbb{Z}_p$ is not divisible by p, then $a \in \mathbb{Z}_p^\times$.

P3. For $a \in \mathbb{F}_p$ and $n \in \mathbb{Z}_{>0}$, the number of solutions $N_p(x^n = a)$ is $\displaystyle\sum_{\chi^d = \mathbb{1}} \chi(a)$, where $d = (n, p-1)$, and the sum is taken over characters χ of $\mathbb{F}_p^\times$ such that $\chi^d = \mathbb{1}$.

P4. Use P3 and Set #9 N2 and P2 to estimate $N_p(x^n + y^n = 1)$. In particular, show that for all p sufficiently large, the equation $x^n + y^n = 1$ has non-trivial solutions (i.e., with x and y both non-zero) modulo p.

Set # 11

Terminology

T1. What is an elliptic curve?

Exploration

E1. Generalize the procedure of Set #9 E2 to define an abelian group law on any non-singular conic in $\mathbb{P}^2$.

E2. Let a be an integer. Is it true that the equation $x^2 = a$ is solvable in $\mathbb{Z}$ if and only if it is solvable in $\mathbb{F}_p$ for all primes p? What about the equation $x^n = a$ for some positive integer n? Formulate a suitable "local-to-global principle" for these equations. Can you generalize your results to $\mathbb{Z}[i]$? To $\mathbb{F}_p[x]$? To $\mathbb{Z}[\sqrt{-5}]$?

E3. In how many points do you "expect" that two plane curves $\{f(x, y) = 0\}$ and $\{g(x, y) = 0\}$ of degrees m and n, respectively, to intersect inside $\mathbb{A}^2(\mathbb{C})$? Make a catalogue of phenomena that can lead to the failure of this expected number of points of intersection.

Numerical Problems (some food for thought)

N1. Over which fields F is the projective curve $Y^2Z = X^3 - 11XZ^2$ non-singular?

N2. Consider the elliptic curve E in N1, equipped with the origin $[0, 1, 0]$, over the field $\mathbb{F}_3$. Describe the abelian group $E(\mathbb{F}_3)$. Do the same for $E(\mathbb{F}_5)$.

N3. Over which fields F is the (projective) cubic curve $3X^3 + 4Y^3 + 5Z^3 = 0$ non-singular? Show that this equation has solutions in $\mathbb{F}_p$ for all primes p (can you use the ideas of Set #10 P3-P4?). Show that the same holds for $\mathbb{Q}_p$ for all primes p (including "$p = \infty$"). Are there any obvious rational solutions?

N4. Repeat N3 with the (affine) curve $2y^2 = x^4 - 17z^4$.

Prove or Disprove and Salvage if Possible

P1. The curve in N4 has no rational solutions other than $(x, y, z) = (0, 0, 0)$. Suitably interpreted (as a curve in "weighted projective space"), this yields an example of the failure of the Hasse Principle! (Hint: use quadratic reciprocity to show that for any prime p dividing y, $\left(\frac{p}{17}\right) = 1$.)

P2. We have now seen two constructions of the p-adic integers $\mathbb{Z}_p$ and the p-adic numbers $\mathbb{Q}_p$, one "algebraic" and the other "analytic." Show that these two constructions yield isomorphic rings (fields).

Set # 12

Terminology

T1. Let $f(x,y), g(x,y) \in \mathbb{C}[x,y]$ be polynomials in two variables, and let $P \in \mathbb{A}^2(\mathbb{C})$ be a point of intersection of the plane curves defined by f and g. What is the intersection multiplicity $I_P(f,g)$ of these curves at the point P? Can you extend this definition to define the intersection multiplicities of two projective curves?

Exploration

E1. Let $F(X_0,\ldots,X_n) \in \mathbb{F}_p[X_0,\ldots,X_n]$ be a degree d homogeneous polynomial over $\mathbb{F}_p$. For instance, you might consider the family of examples $F(X_0,\ldots,X_n) = X_0^d + X_1^d + \ldots + X_n^d$. In this special case, can you find n and d such that $\{F = 0\}$ has no solutions in $\mathbb{P}^2(\mathbb{F}_p)$? If n is large enough compared to d, will $\{F = 0\}$ always have solutions over $\mathbb{F}_p$?

Numerical Problems (some food for thought)

N1. For all points of intersection P of the following affine curves $\{f = 0\}$ and $\{g = 0\}$ inside $\mathbb{A}^2(\mathbb{C})$, compute the intersection multiplicities $I_P(f,g)$.
   (a) $f(x,y) = y - x^2$, $g(x,y) = y$.
   (b) $f(x,y) = x^2 + (y-1)^2 - 1$, $g(x,y) = y - x^2$.
   Do these curves intersect at all in the line at infinity? Compute the sum $\sum_P I_P(f,g)$, taking into account any intersections at infinity, if necessary.

N2. For all points of intersection P of the following projective curves $\{F = 0\}$ and $\{G = 0\}$ inside $\mathbb{P}^2(\mathbb{C})$, compute the intersection multiplicities $I_P(F,G)$, and the sum $\sum_P I_P(F,G)$.
   (a) $F(X,Y,Z) = X - Z$, $G(X,Y,Z) = YZ - X^2$.
   (b) $F(X,Y,Z) = YZ + X^2$, $G(X,Y,Z) = YZ - X^2$.

Prove or Disprove and Salvage if Possible

P1. In this problem, work over the complex numbers. Let F be a non-singular homogeneous polynomial of degree m, and let G be a homogeneous linear polynomial, and write $V(F)$ and $V(G)$ for the corresponding curves in $\mathbb{P}^2(\mathbb{C})$. Then

$$m = \sum_{P \in V(F) \cap V(G)} I_P(F,G).$$

P2. Use Bézout's theorem to give another proof of associativity of the group law on a non-singular conic in $\mathbb{P}^2$.

P3. Use Bézout's theorem to show that if two cubic curves in $\mathbb{P}^2$ intersect in exactly nine points, then any cubic curve passing through eight of the nine points must pass through the ninth as well.

P4. The group law on an elliptic curve in $\mathbb{P}^2$ is associative.