Drexel University, Department of Mathematics

Math 533: Abstract Algebra I, Winter 2021: Homework 0

Darij Grinberg

January 16, 2023

1 Exercise 1

1.1 Problem

How many semesters (or quarters) of abstract algebra have you taken (include Galois theory, representation theory, group theory)?

1.2 Solution sketch

I've gotten answers ranging from 1 to 5.

2 Exercise 2

2.1 Problem

How familiar are you with the notions of

1. ring;

2. normal subgroup of a group;
3. Jordan canonical form (aka Jordan normal form) of a matrix;
4. quotient vector space V/W;
5. exact sequence;
6. determinant;
7. Cayley–Hamilton theorem;
8. greatest common divisor of two (univariate) polynomials;
9. complex number;
10. Gaussian integer;
11. primitive n-th root of unity;
12. discrete Fourier transform?

(Write in a number between 0 (for "never seen it") and 5 (for "remember the important properties and could recall their proofs in 15 minutes without looking up") for each one.)

2.2 Solution sketch

Here are the answers I got, with some comments of mine:

1. ring: 4, 0, 5, 3, 4, 5, 3, 3, 3, 5, 5, 1.

   Some spread here (but hopefully not so much any more now).

2. normal subgroup of a group: 3, 3, 3, 3, 4, 2, 2, 3, 2, 5, 5, 2.

   I asked this one to assess how much you remembered of group theory. I don't actually think normal subgroups will appear in this course (except in the trivial sense: every subgroup of an abelian group is normal).

3. Jordan canonical form (aka Jordan normal form) of a matrix: 4, 5, 5, 5, 5, 4, 4, 3, 3, 5, 5, 4.

   Nice! This should make the rational canonical form (which is a generalization of the Jordan normal form to fields that are not algebraically closed) much less mysterious.

4. quotient vector space V/W: 3, 0, 0, 1, 3, 1, 1, 1, 2, 5, 1, 0.

   Had you done your undergrad in Germany, you would have seen it in your first semester :)

   Quotient vector spaces are "like $\mathbb{Z}/n$ but for vector spaces". We'll soon learn about quotient rings and quotient modules; quotient vector spaces are a particular case of the latter.

5. exact sequence: 1, 2, 0, 0, 2, 0, 1, 0, 1, 4, 1, 0.

   If exact sequences are to appear in this course (and that's an "if"), it will be the short ones only. Their proper habitat is courses on homological algebra and algebraic topology.

6. determinant: 5, 5, 5, 5, 5, 5, 4, 4, 4, 5, 5, 5.

   Reassuring!

7. Cayley–Hamilton theorem: 4, 4, 5, 4, 5, 4, 4, 1, 3, 5, 5, 4.

   I don't expect anyone to remember the proof – at least not the algebraic one.

8. greatest common divisor of two (univariate) polynomials: 4, 1, 3, 4, 3, 4, 4, 4, 5, 5, 2, 3.

   This will come useful to us pretty soon.

9. complex number: 5, 3.5, 5, 4, 5, 5, 4, 4, 4, 5, 5, 4.

   Very nice.

10. Gaussian integer: 0, 2, 5, 2, 1, 1, 1, 0, 4, 3, 1, 1.

    Should be more now. The Gaussian integers are one of the nicest rings around as far as good properties are concerned, and we'll soon see how they can be used.

11. primitive n-th root of unity: 3, 3, 5, 2, 4, 5, 4, 3, 3, 5, 0, 3.

    There are conflicting definitions of a "primitive n-th root of unity" in the literature. The one I prefer (alas, not the one in Dummit and Foote) is the following: A *primitive n-th root of unity* in a field means an element x of the field such that $x^n = 1$ while the $n-1$ powers $x^1, x^2, \ldots, x^{n-1}$ are distinct from 1. For example, the imaginary unit i of the field $\mathbb{C}$ is a primitive 4-th root of unity.

12. discrete Fourier transform: 1, 0, 3, 1, 3, 1, 2, 1, 0, 5, 0, 2.

    Not sure if I'll get there in this course, but it is a nice application of the n-th roots of unity.

---

3 Exercise 3

3.1 Problem

(a) Factor the polynomial $a^3 + b^3 + c^3 - 3abc$.

(b) Factor the polynomial $bc\,(b-c) + ca\,(c-a) + ab\,(a-b)$.

(c) How general have your methods been? Did you use tricks specific to the given polynomials, or do you have an algorithm for factoring any polynomial (say, with integer coefficients)?

3.2 Solution sketch

(a) The answer is

$$a^3+b^3+c^3-3abc=(a+b+c)\left(a^2+b^2+c^2-bc-ca-ab\right).$$

This is if you want to factor the polynomial over $\mathbb{Z}$ (i.e., into polynomials with integer coefficients). Over $\mathbb{C}$, you can factor it further:

$$a^3+b^3+c^3-3abc=(a+b+c)\left(a+\zeta b+\zeta^2 c\right)\left(a+\zeta^2 b+\zeta c\right),$$

where $\zeta=e^{2\pi i/3}=\dfrac{-1+\sqrt{3}i}{2}$.

(b) The answer is

$$bc\,(b-c)+ca\,(c-a)+ab\,(a-b)=(a-b)\,(a-c)\,(b-c).$$

(c) All of the above factorizations can be found using specialized tricks:

For instance, in part **(a)**, it helps to rewrite $a^3+b^3+c^3-3abc$ in terms of the three *elementary symmetric polynomials* $e_1=a+b+c$, $e_2=ab+ac+bc$ and $e_3=abc$ (it is a famous result of Gauss that any symmetric polynomial in a,b,c can be expressed as a polynomial in e_1,e_2,e_3, and there is an algorithm that finds such an expression); once this is done, the $a+b+c$ factor immediately leaps to the eye. The other factor, $a^2+b^2+c^2-bc-ca-ab$, is irreducible over $\mathbb{Z}$ (you can check this easily by substituting distinct constants for b and c and checking that the resulting quadratic in a has no real roots); over $\mathbb{C}$ you can factor it using the usual methods for solving quadratic equations (treating b and c as constants).

I discussed ways of finding the factorization in **(b)** on `https://math.stackexchange.com/a/3127648/` . The simplest one is to observe that the polynomial vanishes for $b=c$ and therefore must be divisible by $b-c$. (Do you see why?)

The more interesting question is how to factor polynomials in general. There is no fully general algorithm for factoring polynomials over an arbitrary field, even if the polynomials are univariate (see `https://mathoverflow.net/a/350877/` for a brief outline). However, Kronecker found an algorithm for factoring polynomials in any number of variables over $\mathbb{Z}$. A brief outline of the algorithm can be found in `https://math.stackexchange.com/a/3127648/` , but you may want to find it yourself. It is based on the following two ideas:

1. If $f\in\mathbb{Z}[x]$ is a polynomial in one variable x with integer coefficients, and if $g\in\mathbb{Z}[x]$ is a polynomial that divides f in $\mathbb{Z}[x]$, then the integer $g(n)$ divides $f(n)$ for each $n\in\mathbb{Z}$. Unless $f=0$, there are only finitely many $n\in\mathbb{Z}$ for which $f(n)=0$.

2. If $f\in\mathbb{Z}[x_1,x_2,\ldots,x_n]$ is a polynomial in $n>1$ variables $x_1,x_2,\ldots,x_n$ with integer coefficients, and if $g\in\mathbb{Z}[x_1,x_2,\ldots,x_n]$ is a polynomial that divides f, then the polynomial $g\left(x_1,x_2,\ldots,x_{n-1},x_{n-1}^k\right)$ divides $f\left(x_1,x_2,\ldots,x_{n-1},x_{n-1}^k\right)$ in the ring $\mathbb{Z}[x_1,x_2,\ldots,x_{n-1}]$ for any $k\in\mathbb{N}$. (Essentially, this is saying that setting $x_n:=x_{n-1}^k$ does not break divisibility.) Can you find a sufficiently high k that ensures the converse also holds?

---

4 Exercise 4

4.1 Problem

Simplify $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$.

4.2 Solution sketch

The answer is 1.

You can find this numerically, but how to prove it?

First proof: One way is to set $u=\sqrt[3]{2+\sqrt{5}}$ and $v=\sqrt[3]{2-\sqrt{5}}$. We must then show that $u+v=1$. The definitions of u and v yield $u^3=2+\sqrt{5}$ and $v^3=2-\sqrt{5}$, so that $u^3+v^3=\left(2+\sqrt{5}\right)+\left(2-\sqrt{5}\right)=4$ and $u^3v^3=\left(2+\sqrt{5}\right)\left(2-\sqrt{5}\right)=4-5=-1$. Hence, $(uv)^3=u^3v^3=-1$, so that $uv=-1$ (here we are taking the cube root, which is unique because u and v are **real** numbers). Now, the binomial formula yields

$$(u+v)^3=u^3+3u^2v+3uv^2+v^3=\underbrace{u^3+v^3}_{=4}+3\underbrace{uv}_{=-1}(u+v)=4-3(u+v).$$

In other words, $u+v$ is a solution of the cubic equation $x^3=4-3x$. How do you solve this cubic equation? If you try to apply Cardano's formula, you get right back to the expression $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$ you started with, which is not very useful. However, if you already know what you are looking for (viz., you want to show that $u+v=1$), you already **know** that 1 is a root of the cubic $x^3-(4-3x)$; polynomial division then shows that $x^3-(4-3x)=(x-1)\left(x+x^2+4\right)$, and this entails that 1 is the **only** real root of this cubic (since the factor $x+x^2+4$ has no real roots). In other words, 1 is the only real solution of the cubic equation $x^3=4-3x$. Since $u+v$ is a solution of this equation, we thus conclude that $u+v=1$, qed.

Remark: If you have no computer to tell you that the answer is conspicuously close to 1, you can still find it using the rational root test, once you suspect that $u+v$ might be rational.

Second proof: A straightforward computation shows that $\left(\frac{1}{2}\left(1+\sqrt{5}\right)\right)^3=2+\sqrt{5}$. Thus, $\sqrt[3]{2+\sqrt{5}}=\frac{1}{2}\left(1+\sqrt{5}\right)$. Similarly, $\sqrt[3]{2-\sqrt{5}}=\frac{1}{2}\left(1-\sqrt{5}\right)$. Adding the latter two equalities together yields $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}=\frac{1}{2}\left(1+\sqrt{5}\right)+\frac{1}{2}\left(1-\sqrt{5}\right)=1$, qed.

Remark: Guessing the identity $\left(\frac{1}{2}\left(1+\sqrt{5}\right)\right)^3=2+\sqrt{5}$ is far from straightforward, however!

5 Exercise 5

5.1 Problem

Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be n integers, and let $b_1, b_2, \ldots, b_n$ be n further integers. The Gaussian elimination tells you how to solve the system

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = 0;$$
$$b_1 x_1 + b_2 x_2 + \cdots + b_n x_n = 0$$

for n unknowns $x_1, x_2, \ldots, x_n \in \mathbb{Q}$. The answer, in general, will have the form "all $\mathbb{Q}$-linear combinations (i.e., linear combinations with rational coefficients) of a certain bunch of vectors". (More precisely, "a certain bunch of vectors" are $n-2$ or $n-1$ or n vectors with rational coordinates, depending on the rank of the $2 \times n$-matrix $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$.)

Now, how can you solve the above system for n unknowns $x_1, x_2, \ldots, x_n \in \mathbb{Z}$? Will the answer still be "all $\mathbb{Z}$-linear combinations (i.e., linear combinations with integer coefficients) of a certain bunch of vectors"?

What about more general systems of linear equations to be solved for integer unknowns?

5.2 Solution sketch

Yes, the answer will still be "all $\mathbb{Z}$-linear combinations (i.e., linear combinations with integer coefficients) of a certain bunch of vectors". We will see why after we have introduced the Smith normal form (a variant of Gaussian elimination for PIDs instead of fields).

---

6 Exercise 6

6.1 Problem

You are given a 4×4-grid of lamps, each of which is either on or off. For example, writing 1 for "on" and 0 for "off", it may look as follows:

1	0	0	1
1	1	0	0
1	0	0	1
0	1	1	1

In a single move, you can toggle any lamp (i.e., turn it on if it was off, or turn it off if it was on); however, this will also toggle every lamp adjacent to it. ("Adjacent to it" means "having a grid edge in common with it"; thus, a lamp will have 2 or 3 or 4 adjacent lamps.) For example, if we toggle the second lamp (from the left) in the topmost row in the above example grid, then we obtain

0	**1**	**1**	1
1	**0**	0	0
1	0	0	1
0	1	1	1

(where the boldfaced numbers correspond to the lamps that have been affected by the move).

Assume that all lamps are initially off. Can you (by a strategically chosen sequence of moves) achieve a state in which all lamps are on?

[*Remark:* You can play this game (albeit with a 5×5-grid) on `https://codepen.io/wintlu/pen/ZJJLGz` .]

6.2 Solution sketch

This is easier than I thought – four moves suffice:

$$\begin{array}{|c|c|c|c|}\hline 0&0&0&0\\\hline 0&0&0&0\\\hline 0&0&0&0\\\hline 0&0&0&0\\\hline\end{array} \to \begin{array}{|c|c|c|c|}\hline \mathbf{1}&\mathbf{1}&\mathbf{1}&0\\\hline 0&\mathbf{1}&0&0\\\hline 0&0&0&0\\\hline 0&0&0&0\\\hline\end{array} \to \begin{array}{|c|c|c|c|}\hline 1&1&1&0\\\hline \mathbf{1}&1&0&0\\\hline \mathbf{1}&\mathbf{1}&0&0\\\hline \mathbf{1}&0&0&0\\\hline\end{array} \to \begin{array}{|c|c|c|c|}\hline 1&1&1&\mathbf{1}\\\hline 1&1&\mathbf{1}&\mathbf{1}\\\hline 1&1&0&\mathbf{1}\\\hline 1&0&0&0\\\hline\end{array} \to \begin{array}{|c|c|c|c|}\hline 1&1&1&1\\\hline 1&1&1&1\\\hline 1&1&\mathbf{1}&1\\\hline 1&\mathbf{1}&\mathbf{1}&\mathbf{1}\\\hline\end{array}.$$

The case of a 5×5-grid is much less obvious, but the answer is still that the desired state can be achieved. The same holds for any $n \times m$-grid, and more generally for any (finite undirected) graph grid. This is an illustration of linear algebra over the finite field $\mathbb{Z}/2$ (that is, linear algebra where the scalars are not real numbers but elements of $\mathbb{Z}/2$). Indeed, a state of our grid can be viewed as a vector over $\mathbb{Z}/2$ (that is, a vector with entries in $\mathbb{Z}/2$); then, a move corresponds to the addition of a certain fixed vector to it. See §6.1.4 in `https://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf` for how to use this model to solve the problem in general. (We'll learn the prerequisites for that solution soon, although many of you probably know them already.)

---

7 Exercise 7

7.1 Problem

(a) How many of the numbers $0, 1, \ldots, 6$ appear as remainders of a perfect square divided by 7 ?

(b) How many of the numbers $0, 1, \ldots, 13$ appear as remainders of a perfect square divided by 14 ?

What about replacing 7 or 14 by n? Can you do better than just squaring them all?

[For example, 3 of the numbers $0, 1, \ldots, 4$ appear as remainders of a perfect square divided by 5 – namely, the three numbers $0, 1, 4$.]

7.2 Solution sketch

We will use the notation $u\%n$ for the remainder obtained when dividing an integer u by a positive integer n. For example, $16\%7 = 2$.

(a) The following table shows the remainders of some perfect squares divided by 7:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$k^2\%7$	0	1	4	2	2	4	1	0	1	4	2	2	4	1

.

You see that these remainders repeat every 7 columns, because $(k+7)^2 \,\%7 = k^2\%7$ for every integer k (this follows from $(k+7)^2 \equiv k^2 \bmod 7$, which in turn is a consequence of $k+7 \equiv k \bmod 7$). Thus, we only need to count the remainders obtained from any 7 consecutive integers – for example, from $0, 1, \ldots, 6$. There are 4 of these remainders (namely, $0, 1, 2, 4$).

(b) The following table shows the remainders of some perfect squares divided by 14:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$k^2\%14$	0	1	4	9	2	11	8	7	8	11	2	9	4	1

.

As in part **(a)**, we see that there are 8 of these remainders (namely, $0, 1, 2, 4, 7, 8, 9, 11$).

Remark: We can simplify our counting by observing the symmetry $(14-k)^2 \,\%14 = k^2\%14$ for each integer k (so it suffices to only scan the first 8 squares $0^2, 1^2, \ldots, 7^2$).

What about the general question: Given a positive integer n, how many of the numbers $0, 1, \ldots, n-1$ appear as remainders of a perfect square divided by n ? Here is an outline of a solution:

1. Rewrite the question as "How many elements of the finite ring $\mathbb{Z}/n$ are squares?". (Here, a *square* means an element of the form a^2, where $a \in \mathbb{Z}/n$.)
2. Solve this question when $n = p^i$ for some prime p and some $i \in \mathbb{N}$. The answers will be different depending on whether p is 2 or not.
3. Use the Chinese Remainder Theorem to solve the case of general n.

Note that the answer will **not** always be $\left\lceil \dfrac{n+1}{2} \right\rceil$, although we got this answer in both parts **(a)** and **(b)** of the problem.

---

8 Exercise 8

8.1 Problem

Solve the following system of equations:

$$a^2 + b + c = 1;$$
$$b^2 + c + a = 1;$$
$$c^2 + a + b = 1$$

for three complex numbers a, b, c.

8.2 Solution sketch

Let (a, b, c) be a solution. Subtracting the equations $a^2 + b + c = 1$ and $b^2 + c + a = 1$ from one another, we obtain

$$a^2 + b - b^2 - a = 0.$$

The left hand side of this equation factors as $(a-b)(a+b-1)$; thus, we have

$$(a-b)(a+b-1)=0.$$

In other words,

$$a-b=0 \text{ or } a+b-1=0.$$

Similarly, we have

$$b-c=0 \text{ or } b+c-1=0.$$

Similarly, we have

$$c-a=0 \text{ or } c+a-1=0.$$

Thus, we are in one of the following eight cases:
Case 1: We have $a-b=0$ and $b-c=0$ and $c-a=0$.
Case 2: We have $a-b=0$ and $b-c=0$ and $c+a-1=0$.
Case 3: We have $a-b=0$ and $b+c-1=0$ and $c-a=0$.
Case 4: We have $a-b=0$ and $b+c-1=0$ and $c+a-1=0$.
Case 5: We have $a+b-1=0$ and $b-c=0$ and $c-a=0$.
Case 6: We have $a+b-1=0$ and $b-c=0$ and $c+a-1=0$.
Case 7: We have $a+b-1=0$ and $b+c-1=0$ and $c-a=0$.
Case 8: We have $a+b-1=0$ and $b+c-1=0$ and $c+a-1=0$.

In each of the eight cases, we are left with a system of 3 linear equations in 3 unknowns, which we can solve. Here are the details:

In Case 1, the system of linear equations yields $a=b=c$. Hence, in our original equation $a^2+b+c=1$, we can replace all three unknowns by c. Thus, we obtain $c^2+c+c=1$. This is a quadratic equation in c, and its solutions are $\sqrt{2}-1$ and $-\sqrt{2}-1$. Hence, we obtain the solutions

$$(a,b,c)=\left(\sqrt{2}-1,\ \sqrt{2}-1,\ \sqrt{2}-1\right) \qquad \text{and}$$
$$(a,b,c)=\left(-\sqrt{2}-1,\ -\sqrt{2}-1,\ -\sqrt{2}-1\right).$$

Check that these two solutions are indeed solutions of the original system!

In Case 2, the system of linear equations yields $(a,b,c)=\left(\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$. However, this does not satisfy the original equation $a^2+b+c=1$. Hence, we do not get any solution in Case 2.

Case 3, too does not contribute any solutions.

In Case 4, the system of linear equations yields $a=1-c$ and $b=1-c$. Hence, in our original equation $a^2+b+c=1$, we can replace the unknowns a and b by $1-c$. Thus, we obtain $(1-c)^2+(1-c)+c=1$. This is a quadratic equation in c, and its solution is 1. Thus, $c=1$ and therefore $a=1-c=1-1=0$ and similarly $b=0$. Hence, we obtain the solution

$$(a,b,c)=(0,0,1).$$

Again, check that this satisfies the original system!

Case 5 does not contribute any solutions.

Cases 6 and 7 contribute the solutions

$$(a,b,c)=(1,0,0) \qquad \text{and} \qquad (a,b,c)=(0,1,0),$$

respectively.

Finally, Case 8 contributes the fake solution $(a,b,c) = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$ (in the sense that the linear equations yield this solution, but it fails to satisfy the original system).

Thus, altogether, our system has the five solutions

$$\left(\sqrt{2}-1,\ \sqrt{2}-1,\ \sqrt{2}-1\right), \qquad \left(-\sqrt{2}-1,\ -\sqrt{2}-1,\ -\sqrt{2}-1\right),$$
$$(1,0,0), \qquad (0,1,0), \qquad (0,0,1).$$

Remark: Systems of polynomial equations in general can be rather hard to solve. The one in this exercise was chosen to be susceptible to a simple trick (as we have seen above); but wiggle one of the coefficients a little bit (e.g., replacing one of the three 1's by a 2), and the answer gets much more complicated. The fact that all three equations are quadratic does not save us: A **system** of quadratic equations can be as complicated as a univariate equation of arbitrarily high degree.

There **is** a general way of solving systems of polynomial equations, assuming that you can solve univariate polynomial equations. This is known as *elimination theory*, and can be done either using resultants or using Gröbner bases (which we should see near the end of the course). Note that this is **not** what we have done in our above solution.

---

9 Exercise 9

9.1 Problem

The following triangular table shows the binomial coefficients $\binom{n}{m}$ for $n \in \{0,1,\ldots,7\}$ and $m \in \{0,1,\ldots,n\}$:

	$k{=}0$	$k{=}1$	$k{=}2$	$k{=}3$	$k{=}4$	$k{=}5$	$k{=}6$	$k{=}7$
$n=0\ \rightarrow$	1							
$n=1\ \rightarrow$	1	1						
$n=2\ \rightarrow$	2	1						
$n=3\ \rightarrow$	3	3	1					
$n=4\ \rightarrow$	6	4	1					
$n=5\ \rightarrow$	10	10	5	1				
$n=6\ \rightarrow$	20	15	6	1				
$n=7\ \rightarrow$	35	35	21	7	1			

(This is part of what is known as *Pascal's triangle*.)

Now, in this table, let us replace each even number by a 0 and each odd number by a 1.

We obtain

							$k=0$ ↙							
$n=0$	→					1		$k=1$ ↙						
$n=1$	→				1		1		$k=2$ ↙					
$n=2$	→			1		0		1		$k=3$ ↙				
$n=3$	→		1		1		1		1		$k=4$ ↙			
$n=4$	→	1		0		0		0		1		$k=5$ ↙		
$n=5$	→		1		1		0		0		1		$k=6$ ↙	
$n=6$	→	1		0		1		0		1		0		1	$k=7$ ↙
$n=7$	→	1		1		1		1		1		1		1	

This looks rather similar to the third evolutionary stage of Sierpinski's triangle:

(Each 0 in the above table corresponds to a white △ triangle, and each 1 corresponds to a black ▲ triangle.)

Where does this similarity come from?

9.2 Solution sketch

See `http://larryriddle.agnesscott.org/ifs/siertri/Pascal.htm` . (Follow the "proof" link for the proof, and then the "proof" link from there to a proof of Lucas's theorem if you want to know. Note that the proof of Lucas's theorem is a beautiful illustration of the usefulness of working with polynomials modulo p – i.e., of working modulo an ideal.)

---

10 Exercise 10

10.1 Problem

A *conic* means a curve of the form

$$\left\{(x,y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 + dx + ey + f = 0\right\},$$

where a, b, c, d, e, f are six real numbers such that $(a,b,c,d,e,f) \neq (0,0,0,0,0,0)$. Examples of conics are

- any circle, e.g., the unit circle $\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$;
- more generally, any ellipse;
- any parabola, e.g., $\{(x,y) \in \mathbb{R}^2 \mid x^2 + y = 0\}$;

- any hyperbola, e.g., $\{(x, y) \in \mathbb{R}^2 \mid xy = 1\}$ or $\{(x, y) \in \mathbb{R}^2 \mid x^2 - y^2 = 1\}$;
- the union of any two lines, e.g., $\{(x, y) \in \mathbb{R}^2 \mid xy = 0\}$.

A conic is said to be *nondegenerate* if it is not the union of two lines.

(a) What is the maximum number of points in which a nondegenerate conic can intersect a line?

(b) What is the maximum number of points in which two nondegenerate conics can intersect each other?

10.2 Solution sketch

(a) The maximum number is 2.

Proof idea. It is easy to see that the value 2 can be achieved (just pick the unit circle as the conic, and the x-axis as the line). It thus remains to prove that a nondegenerate conic always intersects a line in at most 2 points.

Indeed, we observe that any invertible affine coordinate transformation (i.e., any invertible coordinate transformation of the form $(x, y) \mapsto (\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \varphi)$, where $\alpha, \beta, \gamma, \delta, \varepsilon, \varphi$ are constants) sends a conic to a conic[1], and sends a line to a line; thus, it sends a nondegenerate conic to a nondegenerate conic.

Now, consider a nondegenerate conic C and a line L. We must prove that C intersects L in at most 2 points.

Indeed, we can always find an invertible affine coordinate transformation that transforms L into the x-axis (in fact, we can even find a congruence transformation with this property). This transformation will transform the nondegenerate conic C into a new nondegenerate conic C'. In order to prove that C intersects L in at most 2 points, it thus suffices to show that C' intersects the x-axis in at most 2 points.

Let the nondegenerate conic C' be given by the equation $P(x, y) = 0$, where the polynomial $P(x, y)$ is $ax^2 + bxy + cy^2 + dx + ey + f$. Then, the intersections of C' with the x-axis are the points $(0, y)$ with $cy^2 + ey + f = 0$. Thus, we see that there are at most 2 such points unless $c = e = f = 0$ (since a nonzero quadratic equation has at most 2 solutions). But the case $c = e = f$ cannot occur, because in this case the polynomial $P(x, y)$ would simplify to $P(x, y) = ax^2 + bxy + dx = x(ax + by + d)$, which would entail that the conic C' is degenerate (in fact, C' is the union of the x-axis with the line with equation $ax + by + d = 0$ in this case). Hence, we conclude that C' intersects the x-axis in at most 2 points. Consequently, undoing our coordinate transformation, we conclude that C intersects L in at most 2 points. This completes the proof.

(b) To be pedantic, the answer is ∞, since you can take two identical nondegenerate conics.

Let's now answer the real question: What is the maximum number of points in which two **distinct** nondegenerate conics can intersect each other?

I claim that this maximum number is 4.

I thought there would be a simple algebraic proof, but I cannot find it now!

Remark: Both parts **(a)** and **(b)** of the problem are particular cases of *Bézout's theorem for algebraic curves in the plane*, which states that two algebraic curves of degrees p and

[1] This is easy to see from the definition of a conic: Essentially, a conic is the set of points at which a given nonzero degree-2 polynomial vanishes. But an affine coordinate transformation sends a degree-2 polynomial to a degree-2 polynomial.

q (in $\mathbb{R}^2$, or in $\mathbb{C}^2$, or more generally in the Cartesian plane F^2 defined over any field F) intersect in at most pq points unless they have a whole algebraic curve in common.