Drexel University, Department of Mathematics

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

Darij Grinberg

January 6, 2025

1 Exercise 1

Omitted.

2 Exercise 2

2.1 Problem

How familiar are you with the notions of

1. normal subgroup of a group;
2. determinant;
3. ring;
4. Cayley–Hamilton theorem;
5. quotient vector space V/W;

6. exact sequence;
7. complex number;
8. Gaussian integer;
9. primitive n-th root of unity;
10. discrete Fourier transform?
11. greatest common divisor of two (univariate) polynomials;
12. tensor product;
13. cyclotomic polynomial;
14. Reed–Muller code;
15. Elkies–Stanley code;
16. Bose–Chaudhuri–Hocquenghem code?

(Write in a number between 0 (for "never seen it") and 5 (for "could teach a lecture about it with no preparation") for each one.)

2.2 Solution sketch

Here are the answers I got, with some comments of mine (modulo my data entry errors):

1. normal subgroup of a group: 4, 4, 4, 4, 3, 1, 5, 4, 4, 4, 5, 3.

   Anyone with ≤ 3 on this should look this one up, as we will use this concept at least as a motivation. More importantly, we will use the concept of a **quotient** of a group G by a subgroup H. When H is "only" a subgroup of G, this quotient (usually called G/H) is just a set with an action of G on it. However, when H is a **normal** subgroup, this quotient G/H also becomes a group, i.e., we can define a multiplication on it by the rule $\overline{g_1} \cdot \overline{g_2} := \overline{g_1 g_2}$ (or, to use more standard notation, $g_1 H \cdot g_2 H := g_1 g_2 H$) without running into ambiguities.

   This is in Chapter 9 of Gallian's *Contemporary Abstract Algebra* (10th edition 2020), but he calls quotient groups "factor groups".

   The analogous concepts for rings are called "ideal" and "quotient ring", and will be two rather crucial concepts in this course.

2. determinant: 1, 4, 2, 4, 5, 5, 5, 4, 4, 5, 5, 3.

   We won't use them much here, but they might come handy in some homework exercises. Since you have seen group theory, I can define them quickly: Let $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in R^{n \times n}$ be an $n \times n$-matrix with entries in a commutative ring R. Then, its **determinant** $\det A$ is an element of R, defined by the formula

$$\det A := \sum_{\sigma \in S_n} \operatorname{sign} \sigma \cdot \underbrace{a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}}_{= \prod_{i=1}^{n} a_{i,\sigma(i)}}.$$

Here, S_n is the n-th symmetric group (i.e., the group of all permutations of $\{1, 2, \ldots, n\}$), and $\operatorname{sign} \sigma$ denotes the sign of a permutation σ (which is 1 if σ is even, and -1 if σ is odd; I called this $(-1)^\sigma$ back in Math 222). You have likely seen and used determinants for matrices with real entries; the case of entries in an arbitrary commutative ring R is similar. All their basic properties such as Laplace expansion, invariance under row/column operations, etc. still hold for commutative rings[1]. In particular, one can show that a square matrix $A \in R^{n \times n}$ is invertible if and only if its determinant $\det A \in R$ is invertible (in R). Determinants have lots of surprising applications; proofs in algebraic combinatorics often boil down to equalities between certain determinants.

One reason why determinants are so useful in abstract algebra is that they survive generalization to commutative rings better than other linear-algebraic tools. A matrix with entries in an arbitrary R cannot always be row-reduced to a row echelon form, so Gaussian elimination doesn't work in general, but determinants are still available.

3. ring: 1, 3, 2, 1, 0, 0, 3, 2, 2, 2, 4, 3.

   Well, here's hoping the numbers will improve over time :)

4. Cayley–Hamilton theorem: 0, 0, 1, 0, 0, 0, 2, 3, 0, 0, 0, 3.

   It's a beautiful result of linear algebra. It says that if you plug a square matrix $A \in R^{n \times n}$ (again, R can be any commutative ring) into its own characteristic polynomial $\chi_A(t) = \det(A - tI_n)$, then you obtain the zero matrix. Here at Drexel, it is probably Math 504 material (but usually only proved for $R = \mathbb{R}$ and $R = \mathbb{C}$).

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

   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.

6. exact sequence: 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0.

   We won't need them, but I was curious. They would appear at the very start of a course on homological algebra (or midway through a first course in algebraic topology).

7. complex number: 4, 5, 3, 3, 9(?), 5, 5, 5, 4, 4, 5, 5.

   Good to see some large numbers here; they will be a recurring example in our class.

8. Gaussian integer: 0, 1, 0, 0, 3, 0, 2, 0, 1, 1, 1, 0, 0, 4.

   A **Gaussian integer** is a complex number $a + bi$ where both a and b are integers (as opposed to arbitrary real numbers). We will learn more about them very soon.

9. primitive n-th root of unity: 0, 0, 0, 0, 0, 1, 0, 0, 3, 1, 0, 5.

   For your culture: There are conflicting definitions of a "primitive n-th root of unity" in the literature. The one I prefer is the following: A **primitive n-th root of unity** in a field[2] 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. More example, the primitive n-th roots in $\mathbb{C}$ are the

[1] For their proofs, see, e.g., Section 12 and Appendix B in: Neil Strickland, *MAS201 Linear Mathematics for Applications*, lecture notes, 28 September 2013. `https://neilstrickland.github.io/linear_maths/`
Note that these proofs are stated for numbers, but work just as well in any commutative ring.

[2] Field = nontrivial commutative ring in which every nonzero element has an inverse.

numbers of the form $e^{2\pi ik/n}$, where $k \in \{1, 2, \ldots, n\}$ is coprime to n. Primitive n-th roots of unity are essential in number theory and applied mathematics, and directly related to the ancient problem of constructing regular n-gons; but I'm not sure if we'll see much of them in this course.

10. discrete Fourier transform: 0, 2, 1, 0, 0, 2, 0, 2, 1, 2, 3, 2.

    I thought I might get to it as an application of primitive n-th roots of unity. At this point, probably unlikely. You might learn about it somewhere else, though.

11. greatest common divisor of two (univariate) polynomials: 1, 0, 0, 2, 0, 0, 0, 1, 2, 1, 2, 0.5.

    OK, I had expected higher numbers here. I'll have to cover this in more detail than I thought.

12. tensor product: 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 3.

    Sadly, won't get there. Hugely important topic, but takes a couple weeks of acclimatization.

13. cyclotomic polynomial: 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

    Another ship passing in the wind; it would fit well if we had another quarter.

14. Reed–Muller code: 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

    I hope to get to this one. It's a nice application of polynomials over finite fields.

15. Elkies–Stanley code: 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

    Good! This was a control question. Elkies and Stanley have both worked in coding theory, but there is no such thing as an Elkies–Stanley code.

16. Bose–Chaudhuri–Hocquenghem code: 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0.

    This one is not a control question; this code (or, rather, these codes – it's a whole class) exists! Another application of polynomials over finite fields, but too advanced to realistically cover in Math 332.

---

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 $\zeta=e^{2\pi i/3}=\dfrac{-1+\sqrt{3}i}{2}$. (This ζ is a primitive 3-rd root of unity, by the way; the three complex numbers $1,\zeta,\zeta^2$ are the vertices of an equilateral triangle when drawn in the plane.)

(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 of the reason why). However, Kronecker found an algorithm for factoring polynomials in any number of variables over $\mathbb{Z}$. This algorithm is outlined in §6.5 of the notes, 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?

This algorithm is mathematically bullet-proof but impractical due to the large numbers that quickly appear. Nevertheless, for the above examples, it shouldn't be too bad (with a modern computer). In practice, computer algebra software uses more efficient algorithms, e.g., using the Chinese Remainder Theorem (which we will see soon!) to "divide-and-conquer" the problem into several more manageable (since small) problems.

---

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 algorithm 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). See Remark 7.1.15 in the notes for some details.

---

6 Exercise 6

6.1 Problem

You are given a 5×5-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	1	0	0	1
1	0	0	1	0
0	1	1	1	1
0	1	0	0	0

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

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

(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 on `https://codepen.io/wintlu/pen/ZJJLGz` .]

6.2 Solution sketch

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.)

See `https://en.wikipedia.org/wiki/Lights_Out_(game)` for more about the game.

---

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 $m \in \{0,1,\ldots,n\}$:

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

																														$k{=}0$
																													$\swarrow$	
$n=0$	$\to$													1														$k{=}1$		
																											$\swarrow$			
$n=1$	$\to$											1				1										$k{=}2$				
																									$\swarrow$					
$n=2$	$\to$								1			0				1						$k{=}3$								
																						$\swarrow$								
$n=3$	$\to$						1			1				1				1					$k{=}4$							
																							$\swarrow$							
$n=4$	$\to$				1			0			0				0				1					$k{=}5$					
																								$\swarrow$						
$n=5$	$\to$			1			1			0			0				1				1					$k{=}6$			
																										$\swarrow$			
$n=6$	$\to$		1			0			1			0			1			0			1						$k{=}7$		
																											$\swarrow$		
$n=7$	$\to$	1			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 $\triangle$ triangle, and each 1 corresponds to a black $\blacktriangle$ 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

The number $\sqrt{2}$ is a root of the polynomial x^2-2. The number $\sqrt{3}$ is a root of the polynomial x^2-3. Can you find a polynomial with integer coefficients that has $\sqrt{2}+\sqrt{3}$ as a root?

Yes, I know about the zero polynomial. Find a better one!

10.2 Solution sketch

A better one is x^4-10x^2+1.

Proof. Let $a := \sqrt{2}+\sqrt{3}$. Then, $a-\sqrt{2} = \sqrt{3}$, so that $\left(a-\sqrt{2}\right)^2 = 3$. Hence, $3 = \left(a-\sqrt{2}\right)^2 = a^2 - 2\sqrt{2}a + 2$. This is equivalent to $a^2 - 1 = 2\sqrt{2}a$. Now squaring this again, we find $\left(a^2-1\right)^2 = 8a^2$. Expanding and bringing everything onto the left hand side, we obtain $a^4 - 10a^2 + 1 = 0$. This completes our proof. $\square$

Incidentally, the polynomial $x^4 - 10x^2 + 1$ has four roots:

$$\sqrt{2}+\sqrt{3}, \qquad \sqrt{2}-\sqrt{3}, \qquad -\sqrt{2}+\sqrt{3}, \qquad -\sqrt{2}-\sqrt{3}.$$

So the three extra roots $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ and $-\sqrt{2}-\sqrt{3}$ are "free-riding" on $\sqrt{2}+\sqrt{3}$. Why is this not surprising? Or is it?[3]

So far, so nice. But many questions suggest themselves:

1. Can we do any better than $x^4 - 10x^2 + 1$? That is, can we find a smaller-degree polynomial with integer coefficients that still has $\sqrt{2}+\sqrt{3}$ as a root?
2. Can we also find such a polynomial for $\sqrt{p}+\sqrt{q}$ where p and q are arbitrary integers?
3. What about $\sqrt[3]{p}+\sqrt[5]{q}$ and more complicated numbers?

These questions are not as easy to answer as the above problem. The answer to Question 1 is "no", but I'm not sure how easy this is to prove[4]. Question 2 is fairly easy (just repeat the above proof with p and q instead of 2 and 3). Question 3 is noticeably trickier, but nevertheless the answer is positive (although the required polynomials are much more complicated). The best answer for $\sqrt[u]{p}+\sqrt[v]{q}$ (where p and q are integers and u and v are positive integers) is a polynomial of degree uv which is most explicitly described as the determinant of a certain complicated matrix[5]. If you want something more elementary, try the $u = 2$ case (i.e., try finding a polynomial for $\sqrt{p}+\sqrt[v]{q}$).

[3]Google "conjugate numbers" for the answer; but a proper understanding of conjugate numbers would require understanding of **Galois theory**.

[4]Of course, if you can prove the above implicit observation that a polynomial with integer coefficients that has $\sqrt{2}+\sqrt{3}$ as a root must also have the three "free riders" $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$ and $-\sqrt{2}-\sqrt{3}$ as roots, then this is pretty clear!

[5]The matrix in question is (depending on your method) either the Sylvester matrix of the two polynomials $t^v - q$ and $(x-t)^u - p$ (in the indeterminate t over the polynomial ring $\mathbb{Z}[x]$), or the Kronecker sum of the companion matrices of the two polynomials $x^u - p$ and $x^v - q$. The first method requires some good familiarity with determinants; the second relies on tensor products. I wish there was something simpler!