SUMMER TERM ABSTRACT ALGEBRA
HANDOUT I: FINITE FIELDS

SAMIR SIKSEK

1. What's this?

This is the first of a handful of abstract algebra handouts for Term 3. You are meant to study them, do the exercises, and discuss them with your tutor group. It's an experiment with a different style of learning. Perhaps this is the correct way to learn mathematics. We want to do three things:

(a) revise Year 1 material;
(b) get ready for Year 2;
(c) rekindle the love and excitement you felt towards mathematics just before you joined Warwick!

Here are some self-study tips:

- Experiment with examples.
- Feel free to google, watch videos, read Wikipedia and online lecture notes, discuss with your friends, ... Do whatever it takes to absorb the material.
- If you get stuck on something, move on and come back to it later. It's important when self-studying not to loiter at the begining of a handout and run out time before you reach the end. For example, Sections 2, 3 and 4 of this handout are revision. Things only start getting interesting in Section 5.
- Lecturers are fallible. These handouts might contain mistakes. So you should think of that as part of the exercise: find the mistakes and correct them. If a mistake is really confusing and you'd like to check me, please send me an email.

2. Rings and fields (revision)

If you are struggling to remember rings and fields, revise Chapters XV and XVI of Introduction to Abstract Algebra lecture notes, or skim through the scans for lectures 14 and 15 of that module (you'll find these on the module's Moodle page). Here are somethings that are helpful to remember.

- An element u in a ring R is a **unit** if there is some $v \in R$ such that $uv = vu = 1$. We say that v is the multiplicative inverse of u and write $v = u^{-1}$.

Date: April 30, 2020.

- Fields are non-zero commutative rings in which every non-zero element is a unit. For example, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ are fields, but $\mathbb{Z}$ is not a field.
- $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

Example 1. Let K be a field. Recall that $K[X]$ denotes the ring of polynomials in X with coefficients in K. It is important to be clear on what is and what is not a polynomial. A polynomial in X with coefficients in K has the form

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \qquad a_i \in K.$$

Expressions such at $1/X$ and $(X+1)/(X^2+1)$ are NOT polynomials. They are rational functions. A rational function is the ratio of two polynomials. Also the expression

$$1 + X + X^2 + X^3 + \cdots$$

is NOT a polynomial. It is an example of a powerseries in X. Polynomials have only finitely many terms.

Let's show that $K[X]$ is not a field. Consider X. This is a non-zero element of $K[X]$. We will show that it doesn't have an multiplicative inverse in $K[X]$. Suppose it does, and let that multiplicative inverse be

$$f = a_0 + a_1 X + \cdots + a_n X^n, \qquad a_i \in K.$$

Then $Xf = 1$. This means

$$0 + a_0 X + a_1 X^2 + \cdots + a_n X^{n+1} = 1 + 0 \cdot X + 0 \cdot X^2 + \cdots + 0 \cdot X^{n+1}.$$

Comparing coefficients, we notice in particular that $1 = 0$, giving a contradiction. Hence X is not a unit in $K[X]$ and so $K[X]$ is not a field.

Exercise 1. Let K be a field. Show that $K[X]^* = K^*$. Before you start, let's think about what is being asked. In any ring R, the set R^* is the unit group of R; i.e. it is the set of units of R. Let $f \in K[X]$. Then f is a unit (i.e. in $K[X]^*$) if and only if there is some $g \in K[X]$ such that $fg = 1$. Start by showing that f and g both have degree 0.

Exercise 2. Show that $\overline{1} + \overline{2}X$ is a unit in $(\mathbb{Z}/4\mathbb{Z})[X]$. Why does this not contradict the previous exercise?

For a prime p, we shall write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$, when we want to stress that it is a field.

Exercise 3. Let p be a prime.

(a) How many monic polynomials of degree n are there in $\mathbb{F}_p[X]$?
(b) How many polynomials of degree at most n are there in $\mathbb{F}_p[X]$?
(c) How many polynomials of degree n are there in $\mathbb{F}_p[X]$?

The answers are p^n, p^{n+1} and $p^{n+1} - p^n$ respectively. What matters is giving your reasoning. [1]

3. The Euclidean algorithm (revision)

In Foundations you saw division with remainder.

(I) Let m, $n \in \mathbb{Z}$ with $n \neq 0$. Then there are unique q, $r \in \mathbb{Z}$ such that

$$m = qn + r, \qquad 0 \leq r < |n|.$$

We call q the **quotient** and r the **remainder** obtained upon dividing m by n.

(II) Let g, $f \in \mathbb{R}[X]$ with $f \neq 0$. Then there are unique q, $r \in \mathbb{R}[X]$ with

$$g = qf + r, \qquad r = 0 \quad \text{or} \quad \deg(r) < \deg(f).$$

We call q the **quotient** and r the **remainder** obtained upon dividing g by f. Some people define the degree of the zero polynomial to be $-\infty$. In that case they can simply write

$$g = qf + r, \qquad \deg(r) < \deg(f).$$

For a proof of (II), see Proposition 7.2 of your Foundations lecture notes. Proposition 7.3 of your Foundations lecture notes says that the same is true if $\mathbb{R}[X]$ is replaced by $\mathbb{Q}[X]$ or $\mathbb{C}[X]$, but not by $\mathbb{Z}[X]$. How do we know that (II) is true if $\mathbb{R}[X]$ is replaced by $\mathbb{Q}[X]$ or $\mathbb{C}[X]$? We can simply read through the proof, and check that. In fact the same proof works for $K[X]$ where K is any field. The proof uses the standard properties of addition, subtraction, multiplication and division that hold in any field, not just $\mathbb{R}$. Let's record that as a theorem.

Theorem 2. *Let K be a field. Let g, $f \in K[X]$ with $f \neq 0$. Then there are q, $r \in K[X]$ with*

$$g = qf + r, \qquad \deg(r) < \deg(f).$$

Here we're following the convention $\deg(0) = -\infty$.

Example 3. Let $f = X^2 + 4X + 3$ and $g = X^4 + X^3 + 3X + 3$ in $\mathbb{F}_5[X]$. You can write $f = \overline{1}X^2 + \overline{4}X + \overline{3}$ and $g = \overline{1}X^4 + \overline{1}X^3 + \overline{3}X + \overline{3}$ if you want, but that's too pedantic for me. The important thing to remember is that we're working with the coefficients modulo 5. We do a long division to work out

[1] If you're stuck, start with $p = 3$ and $n = 2$. A monic polynomial of degree 2 in $\mathbb{F}_3[X]$ has the form $X^2 + a_1X + a_0$ where a_0, $a_1 \in \mathbb{F}_3$. There are three possibilities for a_0 and three possibilities for a_1.

the quotient and remainder we obtain on dividing g by f:

$$\begin{array}{rl|llll} & & & X^2 & +2X & +4 \\ \hline X^2+4X+3 &) & X^4 & +X^3 & +3X & +3 \\ & & X^4 & +4X^3 & +3X^2 & \\ \hline & & 2X^3 & +2X^2 & +3X & +3 \\ & & 2X^3 & +3X^2 & +X & \\ \hline & & & 4X^2 & +2X & +3 \\ & & & 4X^2 & +X & +2 \\ \hline & & & & X & +1 \end{array}$$

Make sure you can follow this calculation, and remember at all times that the coefficients are in $\mathbb{F}_5$. Hence the quotient is $q = X^2 + 2X + 4$ and the remainder is $r = X + 1$.

Exercise 4. Your turn! Let

$$f = X^3 + X + 1, \qquad g = X^5 + X^2 + 3$$

in $\mathbb{F}_7[X]$. Workout the quotient and remainder you obtain on dividing g by f.

Both (I) and (II) are the initial steps in Euclid's algorithm for computing the gcd (also called hcf), in $\mathbb{Z}$ and in $K[X]$. The following two theorems are among the most important consequences of Euclid's algorithm.

Theorem 4. *Let m, $n \in \mathbb{Z}$ (not both zero) and let $h = \gcd(m, n)$. Then there are u, $v \in \mathbb{Z}$ such that*

$$h = um + vn. \tag{1}$$

Theorem 5. *Let K be a field. Let f, $g \in K[X]$ (not both zero) and let $h = \gcd(f, g)$. Then there are u, $v \in K[X]$ such that*

$$h = uf + vg. \tag{2}$$

The identities (1) and (2) are often called Bezout identities. It's important to know how to determine the coefficients u, v. If you don't remmeber, revise Section 3.2 of your Foundations lecture notes (the extended Euclidean algorithm). You might also want to look at the Wikipedia pages:

- `https://en.wikipedia.org/wiki/Euclidean_algorithm`
- `https://en.wikipedia.org/wiki/Polynomial_greatest_common_divisor`

Example 6. Let f, g be as in Example 3. Let's follow the steps of the Euclidean algorithm to determine the gcd h and the coefficients u, v. We worked out that

$$X^4 + X^3 + 3X + 3 = (X^2 + 2X + 4)(X^2 + 4X + 3) + (X + 1). \tag{3}$$

Next we divide $X^2 + 4X + 3$ by $X + 1$ to obtain (you do the long division)

$$X^2 + 4X + 3 = (X + 3)(X + 1) + 0.$$

Since the last remainder is 0 we know that the gcd of f and g is the previous remainder which is $X+1$. From (3)

$$\begin{aligned}\underbrace{X+1}_{h} &= 1\cdot(X^4+X^3+3X+3)-(X^2+2X+4)(X^2+4X+3)\\ &= \underbrace{(4X^2+3X+1)}_{u}\underbrace{(X^2+4X+3)}_{f}+\underbrace{1}_{v}\cdot\underbrace{(X^4+X^3+3X+3)}_{g}.\end{aligned}$$

4. Quotients (revision)

One of topics we studied in Introduction to Abstract Algebra is quotients of additive abelian groups (Chapter XIII of the lecture notes, or lecture scan 9). If G is an additive abelian group and H is a subgroup then G/H is the set of cosets of H in G

$$G/H = \{g+H \ : \ g\in G\}.$$

We call $g+H$ the class of g modulo H and frequently denote this by $\overline{g}$. Recall

$$\overline{g_1}=\overline{g_2} \quad\iff\quad g_1-g_2\in H, \tag{4}$$

and that G/H is an additive abelian group where addition is given by

$$\overline{g_1}+\overline{g_2}=\overline{g_1+g_2}.$$

There is a subtlety here: is this operation "well-defined"? We explained and checked this in Introduction to Abstract Algebra.

You know how to do computations in $\mathbb{R}/\mathbb{Z}$ and in $\mathbb{Z}/m\mathbb{Z}$. You also know that $\mathbb{Z}/m\mathbb{Z}$ is not just an additive group, but also a ring. Addition and multiplication make sense in $\mathbb{Z}/m\mathbb{Z}$ and they satisfy the usual commutative ring properties where $\overline{0}=0+m\mathbb{Z}$ is the additive identity and $\overline{1}=1+m\mathbb{Z}$ is the multiplicative identity. Recall what equality in $\mathbb{Z}/m\mathbb{Z}$ means:

$$\begin{aligned}\overline{u}=\overline{v} &\iff u-v\in m\mathbb{Z}\\ &\iff m\mid(u-v)\\ &\iff u\equiv v \pmod m.\end{aligned}$$

Remember how we add and multiply $\overline{a}$ and $\overline{b}$ in practice. We just do these operations in $\mathbb{Z}$, and then take the remainder on dividing the result by m.

Theorem 7. *Addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are well-defined.*

Proof. What does it mean when we say a binary operation is well-defined? It's actually best to start by recalling that multiplication does not make sense in $\mathbb{R}/\mathbb{Z}$. For example, in $\mathbb{R}/\mathbb{Z}$,

$$\overline{1.5}=\overline{0.5}, \qquad \overline{1.1}=\overline{0.1}.$$

However,

$$\overline{1.5\times 1.1}=\overline{1.65}=\overline{0.65}, \qquad \overline{0.5\times 0.1}=\overline{0.05}\neq\overline{0.65}.$$

If we try to define multiplication on $\mathbb{R}/\mathbb{Z}$ by the rule

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

then we run into trouble. We can have $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ but $\overline{a_1 b_1} \neq \overline{a_2 b_2}$. We say that multiplication is not well-defined in $\mathbb{R}/\mathbb{Z}$.

What do we mean when we say multiplication is well-defined in $\mathbb{Z}/m\mathbb{Z}$? We mean precisely that if $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ then $\overline{a_1 b_1} = \overline{a_2 b_2}$. Let's check this. As $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ we know that

$$m \mid (a_1 - a_2), \qquad m \mid (b_1 - b_2).$$

This is the same as

$$a_1 = a_2 + km, \qquad b_1 = b_2 + \ell m, \qquad k,\ \ell \in \mathbb{Z}.$$

Thus

$$a_1 b_1 = (a_2 + km)(b_2 + \ell m) = a_2 b_2 + \underbrace{(kb_2 + \ell a_2 + k\ell m)}_{\in \mathbb{Z}} \cdot m.$$

Hence

$$m \mid (a_1 b_1 - a_2 b_2),$$

which gives the desired $\overline{a_1 b_1} = \overline{a_2 b_2}$.

I'll leave you to check that addition is well-defined in $\mathbb{Z}/m\mathbb{Z}$. □

Exercise 5. Check that addition is well-defined in $\mathbb{Z}/m\mathbb{Z}$. Of course you could say that we have already showed that addition for quotients of additive abelian groups is well-defined (Lemma XIII.17 of Introduction to Abstract Algebra). But it's good to write out the argument again. Try to follow the steps in the proof of Theorem 7.

Let's summarise some basic facts about $\mathbb{Z}/m\mathbb{Z}$.

Theorem 8. *Let $m \geq 2$.*

(a) *$\mathbb{Z}/m\mathbb{Z}$ is a commutative ring.*
(b) *$(\mathbb{Z}/m\mathbb{Z})^* = \{\overline{a} \ : \ a \in \mathbb{Z}$ and $\gcd(a, m) = 1\}$.*
(c) *$\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime.*

Proof. This was covered in Introduction to Abstract Algebra. But it is important to understand this, so we will revise the proofs of (b) and (c). We start with (b). Suppose $\gcd(a, m) = 1$. Then, by Theorem 4 there are u, $v \in \mathbb{Z}$ such that $ua + vm = 1$. Hence $\overline{u} \cdot \overline{a} = \overline{1}$ in $\mathbb{Z}/m\mathbb{Z}$. Therefore $\overline{a}$ is a unit and so belongs to $(\mathbb{Z}/m\mathbb{Z})^*$.

Suppose next that $a \in \mathbb{Z}$ such that $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. We want to show that $\gcd(a, m) = 1$. Since $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$ there $\overline{b}$ such that $\overline{a}\overline{b} = \overline{1}$. This is the same as saying $ab - 1$ is divisible by m. So $ab - 1 = km$ for some $k \in \mathbb{Z}$. Let $t = \gcd(a, m)$. Then t divides a and t divides m. So t divides $1 = ab - km$. Hence $\gcd(a, m) = t = 1$.

We now prove (c). What are we trying to show? What's a field? A field is a non-zero commutative ring where every non-zero element is a unit (i.e. has a multiplicative inverse). Suppose m is prime. Let $\overline{a} \neq \overline{0}$ in $\mathbb{Z}/m\mathbb{Z}$. Then $m \nmid a$. As m is prime, we have $\gcd(m, a) = 1$. Hence by (b), $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. Therefore every non-zero element of $\mathbb{Z}/m\mathbb{Z}$ is a unit and and so $\mathbb{Z}/m\mathbb{Z}$ is a field. Let's do the converse. We want to show that if m is composite then $\mathbb{Z}/m\mathbb{Z}$ is not a field. Well if m is composite then $m = m_1 m_2$ where $1 < m_1 < m$ and $1 < m_2 < m$. Thus $\overline{m_1} \neq \overline{0}$ and $\gcd(m_1, m) = m_1 \neq 1$ so $\overline{m_1}$ is non-zero but not a unit. Hence $\mathbb{Z}/m\mathbb{Z}$ is not a field if m is composite. □

Exercise 6. The proof of Theorem 8 in fact gives a method for computing inverses in $\mathbb{Z}/m\mathbb{Z}$. To check that $\overline{a}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ we check that $\gcd(a, m) = 1$. To compute the inverse all we do is find u, v, using Euclid's algorithm, so that $ua + vm = 1$. Then $\overline{a}^{-1} = \overline{u}$. Compute $\overline{5}^{-1}$ in $\mathbb{Z}/17\mathbb{Z}$.

5. Quotients of Polynomial Rings

Now let K be a field and f be an element of $K[X]$ with positive degree. Write

$$fK[X] = \{fg : g \in K[X]\}.$$

This is the set of polynomials with f as a factor. Note the analogy with

$$m\mathbb{Z} = \{mn : n \in \mathbb{Z}\},$$

which is the set of integers having m as a factor. You've guessed what is coming next. It's easy to check that $fK[X]$ is a subgroup of the additive abelian group $K[X]$. We can take quotient group

$$K[X]/fK[X].$$

For g_1, $g_2 \in K[X]$, we say that $g_1 \equiv g_2 \pmod{f}$ if and only if $f \mid (g_1 - g_2)$. Note the meaning of equality in $K[X]/fK[X]$:

$$\begin{aligned} \overline{u} = \overline{v} &\iff u - v \in fK[X] \\ &\iff f \mid (u - v) \\ &\iff u \equiv v \pmod{f}. \end{aligned}$$

Addition and multiplication in $K[X]/fK[X]$ are defined in the obvious way,

$$\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2}, \qquad \overline{g_1} \cdot \overline{g_2} = \overline{g_1 g_2}.$$

Exercise 7. Check that addition and multiplication are well-defined in $K[X]/fK[X]$. If you get stuck look again at the proof of Theorem 7.

We recall also that every element of $\mathbb{Z}/m\mathbb{Z}$ has a 'canonical form'. It must be equal to a unique class $\overline{r} = r + m\mathbb{Z}$ where $r = 0, 1, \ldots, m - 1$. Given $\overline{a}$ in $\mathbb{Z}/m\mathbb{Z}$ we obtain the canonical form $\overline{r} = \overline{a}$ by simply writing $a = qm + r$ (using division with remainder) where q, $r \in \mathbb{Z}$ and $0 \leq r < m$. Division

with remainder works in $K[X]$ and gives us a canonical form for elements of $K[X]/fK[X]$.

Lemma 9. *Let K be a field and $f \in K[X]$ with $\deg(f) = n \geq 1$. Every element $\overline{g} \in K[X]/fK[X]$ is equal to $\overline{r} = r + fK[X]$ for some unique $r \in K[X]$ with $\deg(r) < \deg(f)$. Moreover, r is the remainder obtained on dividing g by f.*

Proof. Using division with remainder we may write $g = qf + r$ where q, $r \in K[X]$ with $\deg(r) < \deg(f)$. Note that $g - r = qf \in fK[X]$ hence $\overline{g} = \overline{r}$. We want to prove uniqueness of r. Suppose $\overline{g} = \overline{s}$ where $s \in K[X]$ and $\deg(s) < \deg(f)$. Since $\overline{r} = \overline{g} = \overline{s}$ we have $f \mid (r-s)$. But $\deg(r-s) < \deg(f)$ since the polynomials r, s have degree $< \deg(f)$. The only polynomial divisible by f that has degree smaller than f is the zero polynomial. Thus $r - s = 0$ and so $r = s$, proving uniqueness. □

Thus when working in $K[X]/fK[X]$ we always simplify by taking the remainder modulo f.

Example 10. Let $f = X^2 + X + 1$, $g_1 = X + 3$ and $g_2 = X - 4$ in $\mathbb{R}[X]$. We will compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{R}[X]/f\mathbb{R}[X]$. By definition, this is the class of

$$g_1 g_2 = (X + 3)(X - 4) = X^2 - X - 12.$$

But we don't stop here. We would like to simplify by dividing $g_1 g_2$ by f and taking the remainder. Note that

$$g_1 g_2 = qf + r, \qquad q = 1, \quad r = -2X - 13$$

where q is the quotient and r is the remainder. So

$$\overline{g_1} \cdot \overline{g_2} = \overline{-2X - 13}$$

in $\mathbb{R}[X]/f\mathbb{R}[X]$.

Example 11. Let $f = X^2 + 2X + 2$, $g_1 = 2X + 3$ and $g_2 = X + 3$ in $\mathbb{F}_7[X]$. We will compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{F}_7[X]/f\mathbb{F}_7[X]$. By definition, this is the class of

$$g_1 g_2 = (2X + 3)(X + 3) = 2X^2 + 9X + 9 = 2X^2 + 2X + 2$$

as the coefficients are in $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. But we don't stop here. We would like to simplify by dividing $g_1 g_2$ by f and taking the remainder. Note that

$$g_1 g_2 = qf + r, \qquad q = 2, \quad r = 5X + 5$$

where q is the quotient and r is the remainder. So

$$\overline{g_1} \cdot \overline{g_2} = \overline{5X + 5}$$

in $\mathbb{F}_7[X]/f\mathbb{F}_7[X]$.

Exercise 8. Your turn! Let $f = X^2 + 2X + 2$, $g_1 = 2X + 3$ and $g_2 = X + 3$ in $\mathbb{F}_5[X]$. Compute $\overline{g_1} \cdot \overline{g_2}$ in $\mathbb{F}_5[X]/f\mathbb{F}_5[X]$.

Exercise 9. Let p be a prime, and let $f \in \mathbb{F}_p[X]$ have degree $n \geq 1$. Compute $\#\mathbb{F}_p[X]/f\mathbb{F}_p[X]$. You will need Lemma 9 and also your answer to Exercise 3. The answer is p^n, but what matters is your justification.

Theorem 12. *Let K be a field and $f \in K[X]$ have degree ≥ 1.*

(a) *$K[X]/fK[X]$ is a commutative ring.*
(b) *$(K[X]/fK[X])^* = \{\overline{g} \ : \ g \in K[X]$ and $\gcd(f,g) = 1\}$.*
(c) *$K[X]/fK[X]$ is a field if and only if f is irreducible.*

Proof. This should remind you of Theorem 8. I recommend that you read the proof of Theorem 8 again, and then try to prove this theorem on your own.

Part (a) is easy to check. For example let's check that multiplication in $K[X]/fK[X]$ is commutative. We want to check that $\overline{g_1}\cdot\overline{g_2} = \overline{g_2}\cdot\overline{g_1}$ for every pair g_1, $g_2 \in K[X]$. By definition of multiplication in $K[X]/fK[X]$, this is the same as checking that $\overline{g_1 g_2} = \overline{g_2 g_1}$. But we already know that $g_1 g_2 = g_2 g_1$ in $K[X]$ (because $K[X]$ is a commutative ring). Hence $\overline{g_1 g_2} = \overline{g_2 g_1}$. You don't want to waste all day on part (a). Let move on.

We think about (b) next. Suppose $\gcd(f,g) = 1$. By Euclid's algorithm (Theorem 5) there are u, $v \in K[X]$ such that $uf + vg = 1$. Hence $\overline{vg} = \overline{1}$ in $K[X]/fK[X]$. Therefore $\overline{g}$ is a unit and so belongs to $(K[X]/fK[X])^*$.

Suppose next that $g \in K[X]$ such that $\overline{g} \in (K[X]/fK[X])^*$. We want to show that $\gcd(f,g) = 1$. Since $\overline{g} \in (K[X]/fK[X])^*$ there exists $\overline{h}$ such that $\overline{g}\overline{h} = \overline{1}$. This is the same as saying $gh - 1$ is divisible by f. So $gh - 1 = kf$ for some $k \in K[X]$. Let $t = \gcd(f,g)$. Then t divides f and t divides g. So t divides $1 = gh - kf$. Hence $t = 1$. This proves (b). [2]

Next we prove (c). Suppose f is irreducible. We want to show that every non-zero element of $K[X]/fK[X]$ is a unit. Let $\overline{g}$ be a non-zero element of $K[X]/fK[X]$. What does it mean to say $\overline{g} \neq \overline{0}$? It doesn't necessarily mean that g has to be non-zero. It means that $f \nmid g$ (see (4)). As f is irreducible, this implies $\gcd(f,g) = 1$. By part (b), $\overline{g}$ is a unit. Hence $K[X]/fK[X]$ is a field. Let's show the converse. Suppose f is reducible. Therefore $f = f_1 f_2$ where $0 < \deg(f_1) < \deg(f)$ and $0 < \deg(f_2) < \deg(f)$. Then $f \nmid f_1$ and so $\overline{f_1} \neq \overline{0}$. Moreover, $\gcd(f, f_1) = f_1 \neq 1$, so $\overline{f_1}$ is not a unit. Hence if f is composite, then $K[X]/fK[X]$ has a non-zero element which is not a unit and so is not a field. $\square$

Exercise 10. The proof of Theorem 12 in fact gives a method for computing inverses in $K[X]/fK[X]$. To check that $\overline{g}$ is a unit in $K[X]/fK[X]$ we check that $\gcd(f,g) = 1$. To compute the inverse all we do is find u, v, using Euclid's algorithm, so that $uf + vg = 1$. Then $\overline{g}^{-1} = \overline{v}$. Compute $\overline{X+1}^{-1}$ in $\mathbb{F}_2[X]/(X^2 + X + 1)\mathbb{F}_2[X]$.

[2] Actually $t \in K[X]$ divides 1 implies that t has degree 0. However, we follow the convention that the gcd of two polynomials is taken to be monic. Thus $t = 1$.

6. Finite Fields

A finite field is (you guessed it) simply a field which has finitely many elements. An example of a finite field is $\mathbb{F}_p$ with p prime.

Is there a field with 4 elements? Note that $\mathbb{Z}/4\mathbb{Z}$ is a ring with 4 elements but it is not a field. Let $f \in \mathbb{F}_2[X]$ be a quadratic polynomial. Then $\mathbb{F}_2[X]/f\mathbb{F}_2[X]$ has $2^2 = 4$ elements. Is this a field? For this to be a field we want f to be irreducible by Theorem 12. Is there an irreducible, quadratic polynomial in $\mathbb{F}_2[X]$? This is easy to discover. A quadratic polynomial in $\mathbb{F}_2[X]$ has the form $a_2X^2 + a_1X + a_0$ where $a_i \in \mathbb{F}_2$ and $a_2 \neq 0$. Thus the only quadratic polynomials are

$$X^2, \qquad X^2 + X, \qquad X^2 + 1, \qquad X^2 + X + 1.$$

The first three are composite:

$$X^2 = X \cdot X, \qquad X^2 + X = X(X + 1), \qquad X^2 + 1 = (X + 1)^2$$

where the last one is true since $2X = 0X = 0$ in $\mathbb{F}_2[X]$. What about $X^2 + X + 1$. That is irreducible. How do we check that? If it factors then it is the product of two degree 1 polynomials (which could be the same). The only degree 1 polynomials in $\mathbb{F}_2[X]$ are X and $X + 1$. We can just do an exhaustive check and convince ourselves that $X^2 + X + 1$ is irreducible. [3] Hence $\mathbb{F}_2[X]/(X^2 + X + 1)$ is a field with 4 elements. We denote this field by $\mathbb{F}_4$.

Here are some facts about finite fields. These are proven in the third year module Galois theory:

- A finite field necessarily has p^n elements, for some prime p, and some $n \geq 1$.
- If two finite fields have the same number of elements p^n then they are isomorphic. We write $\mathbb{F}_{p^n}$ for any finite field with p^n elements.
- $\mathbb{F}_{p^n}$ is an $\mathbb{F}_p$-vector space of dimension n (more on this below).
- The unit group $\mathbb{F}_{p^n}^*$ is cyclic.

Finite fields are important both to coding theory and to cryptography. If you're intrigued, you might start by looking up the Diffie–Hellman key exchange.

Exercise 11. A finite field with p^n elements is denoted by $\mathbb{F}_{p^n}$. Let $\alpha \in \mathbb{F}_{p^n}$. Show that $\alpha^{p^n} = \alpha$. Hint: of course this is true for $\alpha = 0$, so you can suppose that $\alpha \in \mathbb{F}_{p^n}^*$, which as you know is a group of order ...

[3] You could also say that a quadratic polynomial is reducible iff it has a root. The only possible roots are 0 and 1 (the elements of $\mathbb{F}_2$). Substituting 0 and 1 in $X^2 + X + 1$ we see that neither is a root. So $X^2 + X + 1$ is irreducible in $\mathbb{F}_2[X]$. Could we instead use the quadratic formula? Not here! Remember that the quadratic formula involves dividing by 2. But $2 = 0$ in $\mathbb{F}_2$, so the quadratic formula will not work.

7. Computing in Finite Fields

Let p be a prime, and let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n. We know that $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ is a field with p^n elements, and we denote this field by $\mathbb{F}_{p^n}$. We want to know how to compute in $\mathbb{F}_{p^n}$. To simplify things, let's write

$$\theta = \overline{X} = X + f\mathbb{F}_p[X].$$

Theorem 13. *Every element of $\mathbb{F}_{p^n}$ can be written uniquely as*

$$c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1} \tag{5}$$

where $c_i \in \mathbb{F}_p$.

Proof. Recall Lemma 9: every element of $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$ has the form $\overline{r}$ for some unique $r \in \mathbb{F}_p[X]$ with degree $\deg(r) < n$. Thus $r = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ where $c_i \in \mathbb{F}_p$. Therefore

$$\overline{r} = c_0 + c_1\overline{X} + \cdots + c_{n-1}\overline{X}^{n-1} = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}.$$

□

The theorem is say that every element of $\mathbb{F}_{p^n}$ can be written as a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with coefficients in $\mathbb{F}_p$, in a unique way. You can now convince yourself that $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_p$, of dimension n, with basis $1, \theta, \ldots, \theta^{n-1}$.

Exercise 12. $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)\mathbb{F}_2[X]$ has four elements 0, 1, θ, $1 + \theta$. Do an addition table and a multiplication table for $\mathbb{F}_4$. I'll help you out with one multiplication. Let's compute $\theta(1 + \theta)$. This is the same as $\theta + \theta^2$. We don't stop here. This must be equal to one of our four canonical representations 0, 1, θ, $1 + \theta$ but we don't know which yet. We want to work that out. Recall $\theta = \overline{X}$. So $\theta + \theta^2 = \overline{X + X^2}$. We do division with remainder: $X^2 + X = 1(X^2 + X + 1) + 1$. Hence $\theta + \theta^2 = 1$.

Let's talk a little bit more about how to do computations in $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/f\mathbb{F}_p[X]$, where $f \in \mathbb{F}_p[X]$ is irreducible of degree n. For simplicity, we will assume that f is monic, and write

$$f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n.$$

Then

$$X^n \equiv -a_0 - a_1X - \cdots - a_{n-1}X^{n-1} \pmod{f}$$

which we can also write as

$$\overline{X}^n = -a_0 - a_1\overline{X} - \cdots - a_{n-1}\overline{X}^{n-1}.$$

This is the same as

$$\theta^n = -a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}. \tag{6}$$

The relation (6) is key to doing multiplication in $\mathbb{F}_{p^n}$. Let

$$\gamma = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \qquad \delta = d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1}$$

be two elements of $\mathbb{F}_{p^n}$ where the coefficients c_i, d_i belong to $\mathbb{F}_p$. Then

$$\gamma + \delta = (c_0 + d_0) + (c_1 + d_1)\theta + \cdots + (c_{n-1} + d_{n-1})\theta^{n-1}.$$

That is, if we're doing addition we simply add the coefficients which are elements of $\mathbb{F}_p$; addition is easy. Now let's think about multiplication

$$\gamma\delta = (c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1})(d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1}).$$

We expand the brackets, and collect like terms. This will give us $\gamma\delta$ as a linear combination of $1, \theta, \theta^2, \ldots, \theta^{2n-2}$ with coefficients in $\mathbb{F}_p$. We want $\gamma\delta$ as a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with coefficients in $\mathbb{F}_p$. If there is a θ^n term then that's easy to eliminate, because relation (6) gives us θ^n in terms of lower powers of θ. What if we find a θ^{n+1} term? Well

$$\begin{aligned}\theta^{n+1} &= \theta(-a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}) \\ &= -a_0\theta - a_1\theta^2 - \cdots - a_{n-2}\theta^{n-1} - a_{n-1}\theta^n \\ &= -a_1\theta - a_1\theta^2 - \cdots - -a_{n-2}\theta^{n-1} - a_{n-1}(-a_0 - a_1\theta - \cdots - a_{n-1}\theta^{n-1}).\end{aligned}$$

Expanding brackets and collecting terms gives us θ^{n+1} as a linear combination of $1, \theta, \ldots, \theta^{n-1}$. We can just keep going. To summarize, to compute products in $\mathbb{F}_{p^n}$ what we need to work out what $\theta^n, \theta^{n+1}, \ldots, \theta^{2n-2}$ are as linear combinations $1, \theta, \ldots, \theta^{n-1}$. Once we have these, we can use them to multiply any two elements of $\mathbb{F}_{p^n}$.

Exercise 13. Let $f = X^3 + 3X + 3 \in \mathbb{F}_5[X]$. Check that f is irreducible [4].

We work in $\mathbb{F}_{5^3} = \mathbb{F}_5[X]/f\mathbb{F}_5[X]$. Here every element is a linear combination of $1, \theta, \theta^2$ with coefficients in $\mathbb{F}_5$. The field $\mathbb{F}_{5^3}$ has 125 elements, and no sane person would want to write out a multiplication table for this field. Write down θ^3 and θ^4 as linear combinations of $1, \theta, \theta^2$. Use this to compute the product

$$(1 + \theta^2)(3 + \theta + \theta^2).$$

I get θ^2, but don't take my word for it. I'm OK with making mistakes myself as I don't have to sit exams anymore.

Exercise 14. Let f be as in Exercise 13. Let

$$T \ : \ \mathbb{F}_{5^3} \to \mathbb{F}_{5^3}, \qquad T(\alpha) = (1 + \theta) \cdot \alpha.$$

(a) Check that T is an $\mathbb{F}_5$-linear transformation.
(b) Show that T is an isomorphism.
(c) Write down the matrix M for T with respect to the basis $1, \theta, \theta^2$.

[4]Hint! Let $f \in K[X]$ where K is a field, and suppose f is quadratic or cubic. Convince yourself that f is reducible in $K[X]$ if and only if f has a root in K. For infinite fields this fact is less useful as we can't run through the elements of K and check them one by one. But for a finite field such as $\mathbb{F}_5$ we can run through the elements and check if they're roots of f. While we're on the subject, if we have a quartic polynomial $f \in K[X]$, then it can be reducible but without having roots in K. Write down an example.

(d) Compute the characteristic polynomial χ of M. Check that $\chi(1+\theta) = 0$. If you want an explanation for this, look up the Cayley–Hamilton theorem.

8. Optional LaTeX exercise

Some of you are learning LaTeXthis term. You might have noticed that the typesetting of the long division is amateurish to say the least. The long division symbol is clumsily made up of a right bracket and a horizontal line, and if you look closely, some of the alignment is not quite right. Here is my LaTeX snippet for the long division:

```
\[
\begin{array}{rllllll}
          &     &     &  & X^2 & +2X &+4\\
          \cline{2-7}
X^2+4X+3 &) & X^4 & +X^3 &     & +3X & +3\\
          &  & X^4 & + 4X^3 & + 3X^2 & & \\
            \cline{3-7}
          &  &     &  2 X^3 & + 2X^2 & +3X & +3\\
          &  &     &  2 X^3 & + 3X^2 &+ X & \\
          \cline{4-7}
          &  &     &        & 4X^2 & +2X & +3\\
          &  &     &        & 4X^2 & +X &+2\\
          \cline{5-7}
          &  &     &         &     & X & +1\\
\end{array}
\]
```

Can you do better? Perhaps you can return to this towards the end of your LaTeX course and improve on it.

9. For serious programmers with tons of spare time

Are you a programmer looking for a serious lockdown programming project? If so, there is a LaTeX long division package (google it). You just give it the two polynomials and it produces the long division. I didn't use that package because I expect it doesn't work over $\mathbb{F}_p$. Could you rewrite this package so it has an $\mathbb{F}_p$ coefficients option?