Algebraic Cryptography
Algebra notes

Definition 1. A *ring* (with identity) is a triple $(R, +, \cdot)$ of a set R with two binary operations $+, \cdot$ (called addition and multiplication) such that $(R, +)$ is an abelian group, multiplication distributes over addition, multiplication is associative, and there is a multiplicative identity. When addition and multiplication are known from context, we just refer to R as the ring (instead of the triple $(R, +, \cdot)$). If multiplication is commutative, R is a *commutative ring*.

Example 2. The simplest example of a ring is $\mathbb{Z}$. Perhaps the next simplest class of examples is $\mathbb{Z}_N := \mathbb{Z}/N\mathbb{Z}$ for $N \in \mathbb{N}$.

It is possible to talk about rings where the multiplication does not have an identity element, but we will not do so here.

Definition 3. A *ring homomorphism* between rings R, R' is a function $\phi : R \to R'$ which preserves addition and multiplication. That is, for all $r, s \in R$,

$$\phi(r + s) = \phi(r) + \phi(s), \quad \text{and} \quad \phi(rs) = \phi(r)\phi(s).$$

If ϕ is:

- injective, ϕ is a *monomorphism*,
- surjective, ϕ is an *epimorphism*,
- bijective, ϕ is an *isomorphism*.
- bijective and $R = S$, ϕ is an *automorphism*.

Example 4. Given a ring R, we may form the *polynomial ring* $R[x]$ in the variable x. Addition and multiplication are as usual for polynomials. Of course, we can also have a polynomial ring in several variables $R[x_1, \ldots, x_n]$.

Example 5. All the examples of rings we have discussed so far are commutative. However, we can also consider the ring $M_n(R)$ of matrices over a ring R. Even if R is commutative, $M_n(R)$ is always noncommutative whenever $n \geq 2$.

Exercise 1. *Prove that for any ring R, the ring $M_n(R)$ is noncommutative whenever $n \geq 2$.*

Definition 6. Given a ring R, a nonzero element $u \in R$ is a *unit* if it is invertible in R. We denote the set of units by R^*, which is a multiplicative group.

Definition 7. A *field* $\mathbb{F}$ is a commutative ring in which every nonzero element has a multiplicative inverse. Equivalently, $\mathbb{F}$ is commutative and $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Example 8. Some familiar fields are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Example 9. Here are the groups of units for the various examples of rings we've discussed.

(a) $\mathbb{Z}^* = \{-1, 1\}$,

(b) $\mathbb{Z}_N^* = \{k \in \mathbb{Z}_N \mid \gcd(k, N) = 1\}$,

(c) $M_n(\mathbb{F})^* = GL_n(\mathbb{F})$.

Definition 10. Given $a, b \in \mathbb{Z}$, we say a *divides* b, denoted $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. (Here we may replace $\mathbb{Z}$ with $\mathbb{N}$ everywhere if we so choose, for if $a, b \in \mathbb{N}$, then $c \in \mathbb{N}$ too.) Of course, this definition may be generalized to any ring R (e.g., polynomial rings). In a field, every nonzero element divides every element of the field.

Definition 11. A natural number $p > 1$ is said to be *prime* if it has no divisors x between $1 < x < p$. Equivalently, $p > 1$ is prime if for any $a, b \in \mathbb{Z}$, whenever p divides ab, either p divides a or p divides b.

Problem 12. Prove the two definitions of prime number given above are actually equivalent.

Example 13. Given a prime number p, $\mathbb{F}_p := \mathbb{Z}_p$

Definition 14. For any field $\mathbb{F}$, and any $x \in \mathbb{F}, n \in \mathbb{N}$, we can define

$$nx := \overbrace{x + \cdots + x}^{n \text{ times}} \qquad (-n)x := \overbrace{(-x) + \cdots + (-x)}^{n \text{ times}}$$

If for some p, $px = 0$ for some $0 \neq x \in \mathbb{F}$ (equivalently, *for every* such x, see exercise below), we say that $\mathbb{F}$ *has characteristic* p Otherwise, we say $\mathbb{F}$ has characteristic zero.

Exercise 2. *Prove that* $px = 0$ *for* some $0 \neq x \in \mathbb{F}$ *if and only if* $py = 0$ *for* every $y \in \mathbb{F}$.

Exercise 3. *Prove that any field either has characteristic zero or characteristic* p*, where* p *is prime. (it cannot have composite characteristic)*

Exercise 4. *Prove that if* $\mathbb{F}$ *has characteristic* p *for some prime, then* $\mathbb{F}$ *contains a copy of* $\mathbb{F}_p$*, and similarly, if* $\mathbb{F}$ *has characteristic zero, then* $\mathbb{F}$ *contains a copy of* $\mathbb{Q}$.

Definition 15. Given fields $\mathbb{K}, \mathbb{F}$, we say that $\mathbb{K}$ is an *extension field* of $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{K}$. In this case, we can view $\mathbb{K}$ as an $\mathbb{F}$-vector space. The dimension of this vector space is called the *degree of* $\mathbb{K}$ *over* $\mathbb{F}$, and is denoted $[\mathbb{K} : \mathbb{F}]$. If the degree of $\mathbb{K}$ over $\mathbb{F}$ is finite, we call $\mathbb{K}$ a *finite extension* of $\mathbb{F}$.

Exercise 5. *Prove that* $[\mathbb{R} : \mathbb{Q}] = \infty$ *(*bonus: *more precisely, the degree is* $2^{\aleph_0} = \mathfrak{c}$*) and* $[\mathbb{C} : \mathbb{R}] = 2$.

Theorem 16. *If* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{E}$*, then* $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}]$.

Proof. Suppose that $\mathcal{V} = \{v_\gamma\}_{\gamma\in\Gamma}$ is a basis for $\mathbb{E}$ over $\mathbb{K}$, and that $\mathcal{W} = \{w_\delta\}_{\delta\in\Delta}$ is a basis for $\mathbb{K}$ over $\mathbb{F}$. We claim that $\mathcal{WV} := \{w_\delta v_\gamma\}_{(\delta,\gamma)\in\Delta\times\Gamma}$ is a basis for $\mathbb{E}$ over $\mathbb{F}$.

We first show this collection $\mathbb{F}$-spans $\mathbb{E}$. Let $e \in \mathbb{E}$. Since $\mathcal{V}$ $\mathbb{K}$-spans $\mathbb{E}$, there are $v_1, \ldots, v_n \in \mathcal{V}$ and $k_1, \ldots, k_n \in \mathbb{K}$ such that

$$e = \sum_{j=1}^{n} k_j v_j.$$

Moreover, since $\mathcal{W}$ $\mathbb{F}$-spans $\mathbb{K}$, for each $k_j \in \mathbb{K}$ there are $f_{j,1}, \ldots, f_{j,m_j} \in \mathbb{F}$ and $w_{j,1}, \ldots, w_{j,m_j} \in \mathcal{W}$ so that

$$k_j = \sum_{i=1}^{m_j} f_{j,i} w_{j,i}.$$

Therefore

$$e = \sum_{j=1}^{n} k_j v_j = \sum_{j=1}^{n}\sum_{i=1}^{m_j} f_{j,i} w_{j,i} v_j \in \operatorname{span} \mathcal{WV}$$

We also show $\mathcal{WV}$ is linearly independent over $\mathbb{F}$. Suppose $\Phi \subseteq \Delta \times \Gamma$ is a finite set. Suppose further that for $(\delta, \gamma) \in \Phi$, there are some $f_{\delta,\gamma} \in \mathbb{F}$ and $w_\delta v_\gamma \in \mathcal{WV}$ so that

$$\sum_{(\delta,\gamma)\in\Phi} f_{\delta,\gamma} w_\delta v_\gamma = 0.$$

For convenience, let Φ_Γ denote the projection of Φ onto the second coordinate. Then the above can be written as

$$\sum_{\gamma\in\Phi_\Gamma} \left(\sum_{(\delta,\gamma)\in\Phi} f_{\delta,\gamma} w_\delta \right) v_\gamma = 0.$$

Since the coefficients $\sum_{(\delta,\gamma)\in\Phi} f_{\delta,\gamma} w_\delta \in \mathbb{K}$ and $\mathcal{V}$ is linearly independent over $\mathbb{K}$, we know that for each $\gamma \in \Phi_\gamma$, the coefficient above is zero. Since $\sum_{(\delta,\gamma)\in\Phi} f_{\delta,\gamma} w_\delta = 0$ and $\mathcal{W}$ is linearly independent over $\mathbb{F}$, each $f_{\delta,\gamma} = 0$. This proves $f_{\delta,\gamma} = 0$ for all $(\delta, \gamma) \in \Phi$. Therefore, $\mathcal{WV}$ is linearly independent over $\mathbb{F}$.

Finally, this shows $\mathcal{WV}$ is a basis for $\mathbb{E}$ over $\mathbb{F}$, and therefore

$$[\mathbb{E} : \mathbb{F}] = |\Delta \times \Gamma| = |\Delta|\,|\Gamma| = [\mathbb{E} : \mathbb{K}]\,[\mathbb{K} : \mathbb{F}]. \qquad \blacksquare$$

Definition 17. Given an element $f \in R[x]$ of a polynomial ring, we say f is *irreducible* if whenever $f = gh$ factors, either g or h is a unit of $R[x]$. Note that this is essentially the definition of *prime* adapted for polynomials.

Exercise 6. *Suppose R is an integral domain (i.e., has no zero divisors). Note that R is a subring of $R[x]$ (by identifying R with the constant polynomials). Prove $(R[x])^* = R^*$ under this identification.*

Example 18. Note that the polynomial $f \in \mathbb{Z}[x]$ given by $f(x) = x^2 + x - 1$ is irreducible over $\mathbb{Z}[x]$ but is reducible over $\mathbb{R}[x]$. Indeed, since f has degree 2, it is reducible if and only if it factors into linear factors if and only if its roots are in the ring. But $f(x) = (x - \varphi)(x + \varphi^{-1})$ where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio, which is irrational since $\sqrt{5}$ is irrational.

Theorem 19. *A monic polynomial $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

The proof of this theorem relies on Gauss's Lemma. We will not prove it here because it is outside our scope, but it is an important and useful fact to know.

Exercise 7. *Prove that if a polynomial $f \in \mathbb{R}[x]$ has odd degree $n > 2$, then f is reducible.*

Definition 20. A field $\mathbb{F}$ is called *algebraically closed* if one of the following equivalent conditions holds.

(a) The only nonconstant irreducible polynomials in $\mathbb{F}[x]$ are linear.

(b) Every nonconstant polynomial factors completely into linear terms in $\mathbb{F}[x]$.

(c) Every polynomial has a root in $\mathbb{F}$.

Exercise 8. *Prove the conditions in the definition of algebraically closed are actually equivalent.*

Theorem 21 (Fundamental Theorem of Algebra)**.** *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

There are a plethora of proofs of this fact. Most of them involve some topology or complex analysis and so lie outside the scope of this course. However, there is a primarily algebraic proof using only the fact about how odd degree polynomials over $\mathbb{R}$ are reducible. Once we cover the Fundamental Theorem of Galois Theory, we can revisit the proof of the Fundamental Theorem of Algebra. Also, on Blackboard I have posted a paper which presents an elementary (but nontrivial) proof of the Fundamental Theorem of Algebra using linear algebra. (Jim, you are welcome to sketch your favorite proof of the FTA if you want in class; it's your choice.)

Definition 22. The *algebraic closure* of a field $\mathbb{F}$, denoted $\overline{\mathbb{F}}$ is the *smallest (up to isomorphism)* algebraically closed field containing $\mathbb{F}$. Note: algebraically closed fields containing $\mathbb{F}$ always exist.

Definition 23. A value α is said to be *algebraic over* $\mathbb{F}$ if it is the root of some polynomial in $\mathbb{F}[x]$. Otherwise, α is said to be *transcendental*.

Example 24. The elements $\sqrt{2}, \varphi := \frac{1+\sqrt{5}}{2}$ are algebraic over $\mathbb{Q}$ because they are roots of x^2-2 and x^2+x-1. On the other hand both π, e are transcendental over $\mathbb{Q}$. This latter fact is not obvious.

Exercise 9. *Explain why "most" elements of $\mathbb{R}$ are transcendental over $\mathbb{Q}$.*

Definition 25. A *(left) ideal* J of a ring R is an additive subgroup of R with the property that $rj \in J$ for every $r \in R$ and $j \in J$. Right ideals are defined similarly. If R is commutative, left and right ideals coincide.

Definition 26. An *integral domain* is a commutative ring which has no *zero divisors*. A nonzero element $a \in R$ is said to be a *zero divisor* if there is a nonzero $b \in R$ such that $ab = 0$.

Example 27. The ring $\mathbb{Z}_N$ is an integral domain if and only if N is prime. Indeed, if N is prime, we know that $\mathbb{Z}_N$ is a field, and hence cannot have zeros divisors because every nonzero element has an inverse. Similarly, if N is composite, then $N = nk$ for some $1 < n, k < N$, but $nk \equiv 0 \pmod{N}$.

Definition 28. A *principal ideal* J of a ring R is an ideal generated by a single element. That is, there is some $x \in J$ so that $J = \langle x \rangle := Rx := \{rx \mid r \in R\}$. An integral domain R is a *principal ideal domain* (PID) if every ideal is principal.

Theorem 29. *The polynomial ring $R[x]$ is a PID if and only if R is a field.*

Exercise 10. *Suppose $\mathbb{F}$ is a field and α is algebraic over $\mathbb{F}$. Prove that the set $J = \{f \in \mathbb{F}[x] \mid \alpha$ is a root of $f\}$ is an ideal of $\mathbb{F}[x]$. Conclude that α has a* minimum polynomial*; that is, a polynomial $m_\alpha \in \mathbb{F}[x]$ so that $m_\alpha(\alpha) = 0$ and whenever $f \in \mathbb{F}[x]$ with $f(\alpha) = 0$, m_α divides f. Note: To make the minimum polynomial unique, we also require that it is* monic*, i.e., the coefficient of the highest degree term is* 1*.*

Definition 30. Let α be algebraic over a field $\mathbb{F}$. The *degree of α over $\mathbb{F}$* is the degree of the minimum polynomial m_α over $\mathbb{F}$. Equivalently, this is the degree $[\mathbb{F}(\alpha) : \mathbb{F}]$ where $\mathbb{F}(\alpha)$ is the smallest field containing $\mathbb{F}$ and α (this always exists). The field $\mathbb{F}(\alpha)$ is the field obtained by *adjoining α to $\mathbb{F}$*.

Exercise 11. *Prove the equivalence in the previous definition. That is, if α is algebraic over $\mathbb{F}$, prove that $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_\alpha$. As a corollary, conclude that $\alpha \in \mathbb{F}$ if and only if $\mathbb{F}(\alpha)$ has degree 1 over $\mathbb{F}$ if and only if $\mathbb{F}(\alpha) = \mathbb{F}$.*

Definition 31. Given a polynomial $f \in \mathbb{F}[x]$ of degree d with roots $\alpha_1, \ldots, \alpha_d$ (either in $\mathbb{F}$ or not), the *splitting field of f* is the finite extension $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$. This is the smallest extension of $\mathbb{F}$ over which f splits into linear factors.

Example 32. The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$. However, $\mathbb{Q}(\sqrt[3]{2})$ is *not* the splitting field of $x^3 - 2$. Why? Because $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ and if ω is a primitive cube root of unity, then $\omega\sqrt[3]{2}$ is a root of x^3-2, but it is not in $\mathbb{Q}(\sqrt[3]{2})$ since it isn't real.

Exercise 12. *Prove that the splitting field of* $x^3 - 2$ *is* $\mathbb{Q}(\omega, \sqrt[3]{2})$ *and that* $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

Exercise 13. *If* $f \in \mathbb{F}[x]$ *is irreducible of degree* d*, what are the minimum and maximum possible degrees of the splitting field of* f *over* $\mathbb{F}$*?*

Problem 33. Let $\mathbb{K}$ be the splitting field of the polynomial $X^3 - 2$ over $\mathbb{F}$. Find the degree of $\mathbb{K}$ if $\mathbb{F}$ is: (a) $\mathbb{R}$, (b) $\mathbb{F}_5$, (c) $\mathbb{F}_7$, (d) $\mathbb{F}_{31}$. You must provide justification for your answers.

Definition 34. The *derivative* (respectively, *partial derivatives*) of a polynomial in one (resp., several) variables are defined using the formula $x^n \mapsto nx^{n-1}$. We don't appeal to the limit definition since this doesn't make sense over general (e.g., finite) fields.

Exercise 14. *If a polynomial* $f(x)$ *has a root* α *of multiplicity* $m \geq 2$ *(ie., has* $(x - \alpha)^m$*, then* α *is also a root of its derivative* $f'(x)$*.*

Problem 35. Prove that a polynomial in $\mathbb{F}_p[x]$ has derivative identically zero if and only if it is the p-th power of a polynomial in $\mathbb{F}_p[x]$. Give a criterion for this to happen.

Exercise 15. *Suppose* $\mathbb{F}$ *is a finite field with* q *elements, which we will henceforth denote* $\mathbb{F}_q$ *(we will prove uniqueness up to isomorphism later). Prove that* $q = p^n$ *for some* $n \in \mathbb{N}$ *and some prime* p*.*

Exercise 16. *Prove that* $\operatorname{lcm}(j, n) = \frac{nj}{\gcd(j,n)}$.

Lemma 36. *Suppose* g *is an element of finite order* n *in a group* G*. Then* g^j *has order* $\frac{n}{\gcd(j,n)}$.

Proof. Let $m \in \mathbb{N}$ Then $(g^j)^m = g^{jm} = e$ if and only if $jm = kn$ for some $k \in \mathbb{N}$. In other words, jm is a multiple of n (and necessarily a common multiple of j, n). The smallest that jm can possibly be is $\operatorname{lcm}(j, n) = \frac{jn}{\gcd(j,n)}$ which occurs precisely when $m := \frac{n}{\gcd(j,n)}$. Therefore $o(g^j) = \frac{n}{\gcd(j,n)}$. ■

Theorem 37. *The group* $\mathbb{F}_q^*$ *is cyclic. Moreover, if* g *is a generator of* $\mathbb{F}_q^*$*, then* g^j *is also a generator if and only if* $\gcd(j, q - 1) = 1$.

Proof. Let $n := \max_{y \in \mathbb{F}_q^*} o(y)$ be the maximum of the orders of the elements in $\mathbb{F}_q^*$. We claim that $o(y)$ divides n for any $y \in \mathbb{F}_q^*$. Indeed, let g be an element of order n, and let $y \in \mathbb{F}_q^*$. Since $\mathbb{F}_q^*$ is abelian, $o(gy) = \operatorname{lcm}(o(g), o(y)) \geq o(g) = n$. At the same time, $o(gy) \leq n$, so $o(gy) = n$. This implies that $\operatorname{lcm}(o(g), o(y)) = n = o(g)$, and therefore $o(y)$ divides $o(g)$.

We now claim that g is a generator of $\mathbb{F}_q^*$. For this, notice that from the previous paragraph $y^n = 1$ for every $y \in \mathbb{F}_q^*$, and so the polynomial $x^n - 1$ has at least $q - 1$ roots. Therefore $n \geq q - 1$ (since a polynomial can't have more roots than its degree). But since $n \leq q - 1$ by Lagrange's theorem, this implies $n = q - 1$. Thus g is a generator of $\mathbb{F}_q^*$. Finally, by the preceding lemma, $o(g^j) = \frac{o(g)}{\gcd(j,o(g))} = \frac{q-1}{\gcd(j,q-1)} = q - 1$ if and only if $\gcd(j, q - 1) = 1$. ■

I proved the theorem in the above manner because I felt it was the cleanest. It is different than the one provided in your book, but they both rely on the key fact that a polynomial of degree d can have at most d roots (because of unique factorization).

Definition 38. The *Euler totient function* $\varphi : \mathbb{N} \to \mathbb{N}$ counts the number of positive integers relatively prime to n that are less than n. That is,

$$\varphi(n) := |\{k \in \mathbb{N} \mid k < n, \gcd(k, n) = 1\}|$$

So the previous theorem says that $\mathbb{F}_q^*$ has $\varphi(q-1)$ generators.

Before we prove that following theorem, it is useful to consider the Frobenius automorphism.

Definition 39. Given a field $\mathbb{F}$ of characteristic p, the map $x \mapsto x^p$ is an automorphism of $\mathbb{F}$ called the *Frobenius automorphism.*

To show the Frobenius automorphism is even a homomorphism, we need the following lemma.

Lemma 40. *$(a+b)^p = a^p + b^p$ in any field of characteristic p.*

Proof. Binomial theorem and $\binom{n}{k}$ is divisible by n whenever $0 < k < n$. ■

Since $(ab)^p = a^p b^p$ in any commutative ring, this along with the above lemma prove that the Frobenius automorphism is actually a homomorphism. It is injective because $\mathbb{F}$ if $a^p = 0$, then $a = 0$ (otherwise we could multiply by $(a^{-1})^p$ to get the contradiction $1 = 0$). Thus the kernel of this homomorphism is trivial and so it is injective. Consequently, the Frobenius automorphism is surjective because it is an injective function from a finite set to itself.

Theorem 41. *If $\mathbb{F}_q$ is a field of q elements, then every element is a root of the polynomial $x^q - x$ and $\mathbb{F}_q$ is precisely the set of roots of that equation. Conversely, for every prime power $q = p^f$, the splitting field over $\mathbb{F}_p$ of the polynomial $x^q - x$ is a field of q elements.*

Proof. Suppose that $\mathbb{F}_q$ is a field with q elements. Clearly 0 is a root of $x^q - x$. Moreover, for every $y \in \mathbb{F}_q^*$, the order of y divides $q-1$ by Lagrange's theorem, and therefore $y^{q-1} - 1 = 0$. Multiplying by y, we find that y is root of $x^q - x$. Thus every element of $\mathbb{F}_q$ is a root of $x^q - x$. Since $x^q - x$ has *at most* q distinct roots (in, say, its splitting field), $\mathbb{F}_q$ exhausts *all* the roots of $x^q - x$.

For the converse, suppose that $q = p^f$ with p prime. Let $\mathbb{K}$ denote the splitting field over $\mathbb{F}_p$ of $x^q - x$. Since the derivative of $x^q - x$ is $qx^{q-1} - 1 = -1$ which has no roots, $x^q - x$ has no repeated roots, and therefore has q distinct roots in $\mathbb{K}$. Thus $\mathbb{K}$ contains at least q elements. But we prove the roots of $x^q - x$ are a field, and thus $\mathbb{K}$ must consist only of these roots (since the splitting field is the smallest field containing all the roots). For this, notice that since the map $x \mapsto x^q$ is just f iterations of the Frobenius map, that the sum or product of roots of $x^q - x$ is also a root (since the Frobenius map is a homomorphism).

Moreover, it is clear that the additive inverse of any root is also a root (handle the cases $p = 2$ and p odd separately). Finally, if α is a nonzero root of $x^q - x$, then multiplying $0 = \alpha - \alpha^q$ by $\alpha^{-(q+1)}$, we find α^{-1} is also a root of $x^q - x$. Thus, the roots form a field. ■

Definition 42. Let $\mathbb{F} \subseteq \mathbb{K}$ be an extension of fields, and let τ be an automorphism of $\mathbb{K}$ which fixes $\mathbb{F}$; that is, $\tau|_{\mathbb{F}} = \mathrm{id}_{\mathbb{F}}$. Then the *fixed field of* τ is the intermediate field $\mathbb{F} \subseteq \mathbb{K}^\tau \subseteq \mathbb{K}$ defined by

$$\mathbb{K}^\tau := \{x \in \mathbb{K} \mid \tau(x) = x\}.$$

Exercise 17. *Let $\mathbb{F} \subseteq \mathbb{K}$ be an extension of fields and $\tau \in \mathrm{Aut}(\mathbb{K})$ an automorphism which fixes $\mathbb{F}$. If α is a root of an irreducible polynomial $f \in \mathbb{F}[x]$, then $\tau(\alpha)$ is a* conjugate *of α over $\mathbb{F}$. That is, $\tau(\alpha)$ is also a root of f.*

Theorem 43. *Let $\mathbb{F}_q$ be the field with $q = p^f$ elements and σ is Frobenius automorphism. Then the fixed field of σ is the prime field, i.e., $\mathbb{F}_q^\sigma = \mathbb{F}_p$. Moreover, the order of σ (in the group $\mathrm{Aut}(\mathbb{F}_q)$) is f.*

Proof. By Fermat's Little Theorem, $\mathbb{F}_p$ is fixed by σ. Conversely, any element of $\mathbb{F}_q$ fixed by σ is a root of $x^p - x$, which has at most p roots. Therefore, $\mathbb{F}_q^\sigma = \mathbb{F}_p$.

Let σ^j denote j iterations of σ. Notice that any element of $\mathbb{K}^{\sigma^j}$ is a root of $x^{p^j} - x$, and so is contained in the field $\mathbb{F}_{p^j}$. Thus the order of σ is at least f. Furthermore, we know the elements of $\mathbb{F}_q$ are all roots of $x^q - x$, and hence $\mathbb{F}_q$ is fixed by σ^f. Thus the order of σ in $\mathrm{Aut}(\mathbb{F}_q)$ is f. ■

Theorem 44. *Suppose $\alpha \in \mathbb{F}_q$ and σ is the Frobenius automorphism. Then the conjugates of α over $\mathbb{F}_p$ are the elements $\sigma^j(\alpha) = \alpha^{p^j}$.*

Proof. Suppose α is root of an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree k. Then $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^k}$. If α' is a conjugate of α over $\mathbb{F}_p$, then $\mathbb{F}(\alpha') \cong \mathbb{F}_{p^k}$ as well, and hence all the conjugates of α are roots of $x^{p^k} - x$. Therefore, since σ takes α to conjugates of α, σ restricts to an automorphism of $\mathbb{F}_{p^k} \cong \mathbb{F}(\alpha)$. By the previous theorem, the order of σ in $\mathrm{Aut}(\mathbb{F}_{p^k}) = k$. Since $\mathbb{F}_{p^k} \cong \mathbb{F}(\alpha)$, that k is also the order of the element α under σ. Therefore, iterating sigma runs through all k conjugates of α. ■

Theorem 45. *The subfields of $\mathbb{F}_{p^f}$ are $\mathbb{F}_{p^d}$ for $d \mid f$. Consequently, adjoining an element of $\mathbb{F}_{p^f}$ to $\mathbb{F}_p$ results in one of these fields.*

Proof. Suppose $\alpha \in \mathbb{F}_{p^f}$ has degree d over $\mathbb{F}_p$. Then $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^d}$, and hence $\mathbb{F}_{p^f}$ is a vector space over $\mathbb{F}_{p^d}$ of some dimension, say n. Therefore $p^f = (p^d)^n = p^{dn}$, and thus $d \mid f$.

Conversely, if $f = dn$, and $\alpha \in \mathbb{F}_{p^d}$, then $\alpha^{p^d} = \alpha$, and hence

$$\alpha^{p^f} = \alpha^{p^{dn}} = \alpha^{(p^d)^n} = (((\alpha^{p^d})^{p^d}) \cdots)^{p^d} = \alpha.$$

■

Theorem 46. *For $q = p^f$, the polynomial $x^q - x$ factors over $\mathbb{F}_p$ into the product of all monic irreducible polynomials of degrees d dividing f.*

Proof. Factor $x^q - x$ over $\mathbb{F}_p$ into monic irreducible polynomials. Let d be the degree of one such polynomial. Then adjoining any root of that polynomial yields a subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_q$ and so $d \mid f$ by the previous theorem.

Now, if α is a root of a monic irreducible polynomial g over $\mathbb{F}_p$ of degree $d \mid f$, then $\mathbb{F}(\alpha) \cong \mathbb{F}_{p^d}$ and a previous theorem proves that this contains all conjugates of α over $\mathbb{F}_p$. By the previous theorem $\mathbb{F}_{p^d} \subseteq \mathbb{F}_q$ Therefore g divides $x^q - x$. ■

Exercise 18. *If f is a prime number, then there are $\frac{p^f - p}{f}$ distinct monic irreducible polynomials of degree f over $\mathbb{F}_p$.*

Proof. By the previous theorem $x^{p^f} - x$ factors over $\mathbb{F}_p$ into monic irreducible polynomials of degrees dividing f, of which the only possibilities are $1, f$ since f is prime. The linear factors correspond exactly the p elements of $\mathbb{F}_p$. If we let n denote the number of irreducible polynomials of degree f, then we must have the degree equality $p^f = nf + p$, whence $n = \frac{p^f - p}{f}$. ■

Exercise 19. *Provide a formula for the number of distinct monic irreducible polynomials of degree f (not necessarily prime) over $\mathbb{F}_p$ in terms of the divisors of f.*

Problem 47. Let $\mathbb{F}_q$ where $q = p^f$ be a finite field, and let g be an irreducible polynomial of degree f over $\mathbb{F}_p$. Then two elements of $\mathbb{F}_q$ can be multiplied or divided in $O(\ln^2 q)$ bit operations. If N is a positive integer, then an element can be raised to the N-th power in $\mathbb{F}_q$ in $O(\ln N \ln^2 q)$ bit operations.

Definition 48. An extension of fields $\mathbb{F} \subseteq \mathbb{K}$ is said to be *normal* if every irreducible polynomial (formal derivative is nonzero) over $\mathbb{F}$ with a root in $\mathbb{K}$ factors completely over $\mathbb{K}$. An extension is said to be *separable* if the minimal polynomial over $\mathbb{F}$ of any element in $\mathbb{K}$ has a nonzero formal derivative. An extension is said to be *algebraic* if it has no transcendental elements. An algebraic extension which is normal and separable is called a Galois extension.

Remark 49. Any extension of a field of characteristic zero is separable, as is any algebraic extension of a finite field. An equivalent characterization of Galois extensions are the splitting fields of separable polynomials.

Definition 50. Let $\mathbb{F} \subseteq \mathbb{K}$ be normal and separable extension of fields. Let $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ denote the subgroup of $\mathrm{Aut}(\mathbb{K})$ which fix the field $\mathbb{F}$. We call this the *Galois group of $\mathbb{K}$ over $\mathbb{F}$*.

Theorem 51 (Fundamental Theorem of Galois Theory)**.** *Let $\mathbb{F} \subseteq \mathbb{K}$ be normal and separable extension of fields. Then there is a natural bijection between subgroups of* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *(i.e., automorphisms of $\mathbb{K}$ which fix $\mathbb{F}$) and intermediate*

fields $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$. *In particular, given a subgroup* G *of* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$, *the map* $G \mapsto \mathbb{K}^G$ *given by*

$$\mathbb{K}^G := \bigcap_{\tau \in G} \mathbb{K}^\tau$$

is a bijection whose inverse is given by $\mathbb{E} \mapsto G_{\mathbb{E}}$ *where*

$$G_{\mathbb{E}} := \{\tau \in \mathrm{Gal}(\mathbb{K}/\mathbb{F}) \mid \mathbb{E} \subseteq \mathbb{K}^\tau\}.$$

Moreover, this bijection takes normal subgroups of $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *to normal extensions of* $\mathbb{F}$ *and vice versa. This bijection is inclusion-reversing. Moreover,* $|G| = [\mathbb{K} : \mathbb{K}^G]$ *and* $|\mathrm{Gal}(\mathbb{K}/\mathbb{F})/G| = [\mathbb{K}^G : \mathbb{F}]$.

Remark 52. In the case when $\mathbb{F} \subseteq \mathbb{K}$ is not a Galois extension, the above correspondence still yields an injective map from subgroups to subfields, and a surjective map in the reverse direction. Unfortunately, the other properties are lost.