M007 NOTES: GALOIS THEORY

ARUN DEBRAY

These notes were taken in School of Hard Knocks's M007 (Galois Theory) class in Winter 2016, taught by Jon Snow. I live-TEXed them using `vim`, so there may be typos; please send questions, comments, complaints, and corrections to a.debray@math.utexas.edu.

CONTENTS

Lecture I.

Basic Field Theory

Galois theory involves studying polynomials over a field, which are ubiquitous in algebra and number theory. So we start with the basics of fields.

Definition 1.1. Recall that a *field* k is a commutative ring with 1 such that $1 \neq 0$ and every nonzero element is invertible, and $1 \neq 0$.

That is: in a field we can add, subtract, multiply, and divide, though as usual we can't divide by zero. A "field homomorphism" (meaning a structure-preserving map) is just a ring homomorphism; we ask to preserve addition and multiplication, and subtraction and division come for free.

Example 1.2.

(1) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all fields.
(2) Let p be prime. Then, $\mathbb{Z}/p$ is a field, called the *finite field of order* p and denoted $\mathbb{F}_p$.

Proof. First, we show $\mathbb{Z}/p$ is an integral domain: if $m \cdot n \equiv 0 \bmod p$, then $m \cdot n = xp$ for some x, so p divides either m or n. Thus, either m or n is 0 in $\mathbb{Z}/p$.

Now, for any nonzero $m \in \mathbb{Z}/p$, consider the multiplication map $\varphi_m \cdot : \mathbb{Z}/p \to \mathbb{Z}/p$ sending $n \mapsto mn$. If $a, b \in \mathbb{Z}/p$ are such that $\varphi_m(a) = \varphi_m(b)$, then $\varphi_m(a-b) = m \cdot (a-b) = 0$. Since m is nonzero and $\mathbb{Z}/p$ is an integral domain, then $a = b$, and so φ_m is injective. Since $\mathbb{Z}/p$ is finite, an injective map from $\mathbb{Z}/p$ to itself is a bijection. Thus, there's a unique $n \in \mathbb{Z}/p$ such that $\varphi_m(n) = 1$, or $1 = mn$. That is, every nonzero element is invertible. ⊠

(3) If k is any field, we can form the *field of rational functions* in k, denoted $k(x)$, to be ratios p/q for polynomials $p, q \in k[x]$ with $q \neq 0$. We'd like them to be "in lowest terms," but this is a clunky definition and it's simpler to just say that two rational functions p/q and p'/q' are the same if we can cross-multiply: $pq' = p'q$.

There's not a whole lot we can say about a field k in total generality, without knowing more about it, but we know $1 \in k$, and therefore $1 + 1 \in k$, and $1 + 1 + 1 \in k$, and so on. These numbers might all be distinct, like for $\mathbb{Q}$, or might not be, like for $\mathbb{F}_p$.

Definition 1.3. The *characteristic* $\operatorname{char}(k)$ of a field k is the smallest multiple of 1 that is equal to 0 in k, or is 0 if no such multiple exists.

For example, $\operatorname{char}(\mathbb{F}_p) = p$, and $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = 0$.

Exercise 1.4. Show that for any field k, $\mathrm{char}(k)$ is either 0 or a prime number.

The characteristic is an important property of a field: many important things in Galois theory are different in the characteristic 0 case and the characteristic p case.

One of the consistent lessons of algebra is to study objects by looking at their homomorphisms. In the case of fields, morphisms are the setting of Galois theory.

Lemma 1.5. *Let $\varphi : k \to K$ be a homomorphism of fields. Then, φ is injective.*

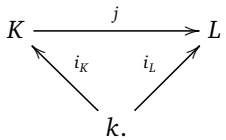
Proof. The kernel $\ker(\varphi) \subset k$ is an ideal of k. Since k is a field, its only ideals are 0 and k itself. If $\ker(\varphi) = 0$, then φ is injective, as desired; if $\ker(\varphi) = k$, then $\varphi(1) = 0$, which is impossible, because ring morphisms must send 1 to 1. ⊠

This is very different than for other kinds of algebraic objects: no interesting kernels and no interesting quotients.

Definition 1.6. If k is a field, a *field extension* of k is a homomorphism $i : k \hookrightarrow L$, often written L/k.[1]

Galois theory is the study of field extensions and relations between them.

Definition 1.7. Let k be a field and $i_K : k \hookrightarrow K$ and $i_L : k \hookrightarrow L$ be field extensions. An *embedding* (sometimes said to be an *embedding over k*) is a field homomorphism $j : K \hookrightarrow L$ such that the following diagram commutes:



That is, $i_L = j \circ i_K$.

Embeddings keep track of how one field lies as a subfield of another.

Definition 1.8. If k is a field, its *prime subfield* is the subfield of k generated by 1.

That is, the prime subfield is the smallest field containing 1 inside k, meaning it must contain $1+1$, $1+1+1$, and so forth. If $\mathrm{char}(k) = 0$, this generates a copy of $\mathbb{Z}$ inside k, and therefore $\mathbb{Q}$ also, since we can invert all nonzero elements of $\mathbb{Z}$. That is, if $\mathrm{char}(k) = 0$, then the prime subfield of k is $\mathbb{Q}$. In the same way, if $\mathrm{char}(k) = p$, then its prime subfield is $\mathbb{F}_p$.

Corollary 1.9. *If K/k is a field extension, then* $\mathrm{char}(k) = \mathrm{char}(K)$.

This is because the prime subfield of K contains the prime subfield of k.

Example 1.10.

(1) Since $\mathbb{Q}$ is a subfield of $\mathbb{R}$, the inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$ is a field extension. In the same way, $\mathbb{R} \hookrightarrow \mathbb{C}$ is a field extension; this fixes $\mathbb{Q}$, so it's an embedding over $\mathbb{Q}$.

(2) The *field of Gaussian rationals* is $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

Exercise 1.11. Show that $\mathbb{Q}(i)$ is a field.

If $a \in \mathbb{Q}$, $a = a + 0i \in \mathbb{Q}(i)$, so $\mathbb{Q} \hookrightarrow \mathbb{Q}(i)$ is another example of a field extension. One can form a similar definition for, e.g. $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{-2})$, but we'll soon define something much more general.

★ **Aside 1.12** (Categorical language in field theory)**.** The modern formulation of abstract algebra tends to use categorical language, defining categories of algebraic objects such that useful constructions satisfy universal properties. However, this is uncommon for field theory, as the category of fields is poorly behaved: few products exist (e.g. the ring $\mathbb{Q} \times \mathbb{Q}$ is not a field), there are no initial or final objects, and the category is disconnected, since a map of fields must preserve the characteristic. Specializing to the category of fields of a given characteristic fixes some, but not all, of these problems.

Nonetheless, there are a few places where words from category theory will simplify things, and I'll try to mention them as they happen. Since they may require knowledge beyond what I assume for these notes, they will also be marked as asides.

[1] This notation looks like a quotient, but since we will never take the quotient by a field extension, this is not ambiguous. We will take quotients of rings, however.

Fixing a base field k, we can define the *category of field extensions* FExt_k to be the category whose objects are field extensions K/k and whose morphisms are embeddings $K \hookrightarrow L$ over k.

TODO: talk about the poset? Eventually will be a lattice.

Lemma 1.13. *If $i : k \hookrightarrow K$ is a field extension, then K is a k-vector space.*

Proof. We need to define an action of k on K, which will just be multiplication: if $\lambda \in k$ and $x \in K$, let $\lambda \cdot x = i(\lambda)x$. The field axioms of K imply (since k is realized as a subfield of K) that multiplication satiafies the axioms for a vector space. ⊠

Definition 1.14. If K/k is a field extension, its *degree*, written $[K : k]$, is the dimension of K as a k-vector space. If this is a finite number, K/k is said to be a *finite extension*; otherwise, it's an *infinite extension*.

This is analogous to the index of a subgroup $[G : H]$. For example, $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}/\mathbb{R}$ is a finite extension, but $\mathbb{R}/\mathbb{Q}$ is an infinite extension.

TODO: treat this in a unified way with adjoining an element; explain what it means to "adjoin a square root of 2," and that this is algebraically indistinguishable (maybe this should be another section, and then irreducibility criteria is a third section).

Irreducibility criteria The key of Theorem 2.2 is that f is irreducible; if we take $k[x]/(f)$ for a reducible f, (f) isn't even prime, so the resulting quotient isn't a field, or even an integral domain! So in practice, we need to know when a polynomial is irreducible. Here are a few criteria.

Lemma 1.15. *If $f \in k[x]$ has degree 2 or 3, then f is irreducible iff it has no roots.*

Of course, the hypothesis is necessary: $(x+2)^2 \in \mathbb{Q}[x]$ is reducible, but has no roots.

Theorem 1.16 (Rational root theorem)**.** *TODO*

Lemma 1.17 (Gauss' lemma)**.** *Let R be a UFD and k be its field of fractions. If $f \in R[x]$, then if f is reducible in $k[x]$, then it's reducible in $R[x]$.*

This is most often used when $R = \mathbb{Z}$, so $k = \mathbb{Q}$: then, it says that *an $f \in \mathbb{Z}[x]$ is irreducible iff it's irreducible in $\mathbb{Q}[x]$.*

Proposition 1.18. *Let R be an integral domain and $I \subset R$ be a proper ideal. If $f \in R[x]$ and $f \bmod I$ is irreducible in $(R/I)[x]$, then f is irreducible over R.*[2]

This is most often used when $R = \mathbb{Z}$ and $I = (p)$ for some prime p.

Proposition 1.19 (Eisenstein's criterion)**.** *Let R be an integral domain and $\mathfrak{p} \subset R$ be a prime ideal. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is such that $a_{n-1}, \ldots, a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$, then f is irreducible in $R[x]$.*

This is generally used for $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for a prime number p. In this case, it says the following.

Corollary 1.20. *Let $f \in \mathbb{Z}[x]$ be given by $f(x) = x^2 + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, and suppose there's a prime number $p \in \mathbb{Z}$ such that $p \mid a_i$ for $i = 0, \ldots, n-1$, and $p^2 \nmid a_0$. Then, f is irreducible in $\mathbb{Z}[x]$.*

By Lemma 1.17, this also implies f is irreducible in $\mathbb{Q}[x]$. The most common application of Eisenstein's criterion is to show that a given polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.

TODO fill in these proofs.

Doing a few exercises using these results will probably be more helpful than reading their proofs.

Proof of Lemma 1.15. If f is reducible, then $f = gh$, where g and h are polynomials of degree at least 1. Since $\deg(g) + \deg(h) \leq 3$, this means at least one of g or h has degree exactly 1. Without loss of generality, assume it's g, so $g(x) = ax + b$ for $a, b \in k$ and $a \neq 0$; then, $-b/a$ is a root of g, and therefore of f.

Conversely, if f has a root, then it's reducible. ⊠

In the next few sections, we'll develop the theory of a few nice kinds of field extensions.

[2] The converse is untrue: $x^4 + 1$ is irreducible over $\mathbb{Z}$, but reducible modulo every prime.

Lecture II.

Adjoining Roots of Polynomials

One of the most important ways to create fields is to adjoin elements. For example, suppose we have $\mathbb{Q}$ already, and we would like to solve $x^2-2=0$. Of course, we can't do that, but we can hope for a solution in an extension field. Certainly, there are two solutions in $\mathbb{R}$, but is there a "minimal" extension $\mathbb{Q}\hookrightarrow K$ such that K has a solution to x^2-2? Creating K from $\mathbb{Q}$ is often called "adjoining a root of 2" or "adjoining a solution to $x^2-2=0$." The minimal such K is $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$. Thus, we care about field extensions in order to understand roots of polynomials: questions about polynomials can be turned into questions about field extensions, which we're going to develop methods to solve.

In this example, we knew already knew of an extension of $\mathbb{Q}$ where x^2-2 had a root, which was helpful. But we don't know that in general: what if we replaced $\mathbb{Q}$ with $\mathbb{F}_5$? Thankfully, we'll prove Theorem 2.2, which says we can abstractly create an extension to adjoin a root of a polynomial over any field. Then, we'll see this produces the same answer as concretely producing an extension inside of a larger field, and that if f is an irreducible polynomial, any two roots of f are "algebraically indistinguishable," in that there extensions given by adjoining those roots are isomorphic.

Soon, we will develop the algebraic closure $\overline{k}$ of a field k, over which every polynomial has a root. Knowing this, one might ask why it's worth developing smaller extensions. Not only do we need these results to develop the algebraic closure, but it's also much easier to do computations in a smaller field extension.

First, though, let's generalize what we did to turn $\mathbb{Q}$ into $\mathbb{Q}(\sqrt{2})$. For the rest of this section, f denotes a nonconstant, irreducible polynomial.

Definition 2.1. Let $k\hookrightarrow K$ be a field extension and $a_1,a_2,\ldots\subset K$. Then, the *field generated by* $a_1,a_2,\ldots$, denoted $k(a_1,a_2,\ldots)$, is the smallest subfield of K containing k as well as a_1, a_2, and so on.

In particular, $k(a_1,a_2,\ldots)$ is an extension of k, and embeds into K. We've already seen that $\sqrt{2}$ and i exist as complex numbers, so we can extend $\mathbb{Q}$ in this way to obtain $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(i)$ or even $\mathbb{Q}(\sqrt{2},i)$.

Theorem 2.2. *Let $f\in k[x]$ be a nonconstant, irreducible polynomial. Then, there's an extension K/k such that f has a root in K.*

Algebraically, what does it actually mean that f has a root in K, given that f is only defined over K? The extension $i:k\hookrightarrow K$ induces a map $i_*:k[x]\hookrightarrow K[x]$ by applying i to each coefficient of a polynomial. Technically, one says that i_*f has a root in K, but there's rarely if ever a need to keep the two separate, so we identify a polynomial with its image over an extension field.

Another way of thinking of this is that a polynomial defines a function: x^2+1, for example, is a function $\mathbb{Q}\to\mathbb{Q}$ that doesn't vanish. However, we can define the same function with the same coefficients on $\mathbb{Q}(i)$, and there it vanishes for $x=\pm i$.

Proof. Since f is nonconstant and irreducible, the ideal $(f)\subset k[x]$ is maximal, and therefore $K=k[x]/(f)$ is a field. Let $j:k\hookrightarrow k[x]$ send $a\in k$ to the constant polynomial a, and $\pi:k[x]\twoheadrightarrow K$ be the canonical projection, taking everything mod (f). Then, $\pi\circ j:k\to K$ is a field homomorphism, so it's an extension.

Finally, we need to produce a root. Consider $\alpha=\pi(x)\in K$. Since π is a ring homomorphism, it commutes with polynomials, and therefore $p(\alpha)=\pi(p(x))$, and this is $p(x)$ mod $p(x)=0$. Hence, α is a root of f. ⊠

We still need to show that the extension K constructed in the proof of Theorem 2.2 is the "smallest," and relate it to Definition 2.1. Fortunately, we can do both things at once: in Theorem 2.4 below, we show that for any extension K of k containing a root a of f, $k(a)\cong k[x]/(f)$ as extensions of k. That is, $k[x]/(f)$ embeds into any extension of k containing a root of f as the subfield that root generates: the extrinsic and intrinsic notions of adjoining an element agree, and are minimal.

★ **Aside 2.3.** Theorem 2.4 can be interpreted in terms of a universal property: given a field extension $k\hookrightarrow K$ and a root $a\in K$ of f, there is a unique map $k[x]/(f)\hookrightarrow K$ sending $x\mapsto a$. Equivalently, $k[x]/(f)$ is initial in the category of pairs (K,a), where K/k is an extension and $a\in K$ is a root of f. This guarantees that the minimal extension is unique up to unique isomorphism if we can construct something satisfying its universal property, and this is exactly what Theorems 2.2 and 2.4 do.

The poset version of this statement might be easier to digest. Inside the poset of field extensions of k (where $K \leq L$ if there's an embedding $K \hookrightarrow L$), we have a sub-poset A of extensions of K containing a root of f. Theorem 2.4 tells us that $k[x]/(f)$ is the minimal element of this poset.

Theorem 2.4. *Let $f \in k[x]$ be a nonconstant, irreducible polynomial and K/k be a field extension containing a root a of f. Then, the assignment $x \mapsto a$ extends to an isomorphism $k[x]/(f) \cong k(a)$ over k.*

Proof. There exists a unique ring homomorphism $\varphi : k[x] \to k(a)$ sending $x \mapsto a$ and a constant polynomial $\lambda \in k$ to $\lambda \in k \hookrightarrow k(a)$. Its kernel is the ideal of polynomials $p \in k[x]$ such that $p(a) = 0$, so $f \in \ker(\varphi)$ and thus $(f) \subseteq \ker(\varphi)$. Thus, φ factors through the quotient, defining a ring homomorphism $\widetilde{\varphi} : k[x]/(f) \to k(a)$. Since both $k[x]/(f)$ and $k(a)$ are fields (the former because f is irreducible), then $\widetilde{\varphi}$ is injective; since k and a are both in $\mathrm{Im}(\widetilde{\varphi})$, then it must be surjective (since they generate $k(a)$ as a ring inside K). Hence, $\widetilde{\varphi}$ is an isomorphism sending $x \mapsto a$; since φ sent constant polynomials to their values in $k \hookrightarrow k(a)$, then so does $\widetilde{\varphi}$, so it is an isomorphism of field extensions of k. ⊠

Thus, even if we don't have an ambient extension $k \hookrightarrow K$, we can still talk about adjoining a root a of f, and call the resulting extension $k(a)$.

Exercise 2.5. There is a third notion of "adjoining an element to a field," which is ring-theoretic. Recall that if R is a subring of a ring S, and $a \in S$, then $R[a]$ is the minimal subring of S containing both R and a. Specializing to fields, consider a finite[3] field extension $k \hookrightarrow K$ and an $a \in K$. Show that $k[a] = k(a)$.

This is why you could "rationalize the denominator" in your high school algebra classes: an element of, say, $\mathbb{Q}(\sqrt{2})$, which may have radicals in the denominator, is equal to an element of $\mathbb{Q}[\sqrt{2}]$, and everything in $\mathbb{Q}[\sqrt{2}]$ is generated by $\mathbb{Q}$ and $\sqrt{2}$ as a ring, meaning we can multiply by $\sqrt{2}$, but not divide: no rationals in the denominator.

Another takeaway of Theorem 2.4 is that, intrinsically, all the roots of an irreducible polynomial "look the same" algebraically: if a and b are both roots of f inside some extension field K, then $k(a) \cong k[x]/(f) \cong k(b)$. For example, this has the curious consequence that if α is one of the complex cube roots of -2, then there's no intrinsic way to distinguish the fields $\mathbb{Q}(\sqrt[3]{-2})$ and $\mathbb{Q}(\alpha)$, even though one consists only of real numbers and the other doesn't.

The takeaway is that some field properties one might find important are actually properties of its embedding inside of a larger field: what distinguishes these two fields is how they sit inside $\mathbb{C}$. The embedding $\mathbb{Q}(\sqrt[3]{-2}) \hookrightarrow \mathbb{C}$ factors through $\mathbb{R} \hookrightarrow \mathbb{C}$, but the embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ does not. It's important to be careful about what's intrinsic versus extrinsic, and for this reason, people often prefer to adjoin elements abstractly, e.g. "let ω denote a cube root of unity and $K = \mathbb{Q}(\omega)$," rather than saying "let $K = \mathbb{Q}((-1 + i\sqrt{3})/2)$," to emphasize that the discussion is true for all three ω satisfying $x^3 - 1 = 0$, rather than for the specific one chosen.

Formally, instead of saying that the roots of an irreducible polynomial "look the same," one says they're *algebraically indistinguishable*. One useful consequence is that it isomorphisms extend: we'll use the following lemma several times, mostly as an ingredient in uniqueness results.

Lemma 2.6 (Extension)**.** *Let $\varphi : K \to L$ be an isomorphism of fields, $f \in K[x]$ be a nonconstant irreducible polynomial, and $g \in L[x]$ be its image under φ. If a is a root of f and b is a root of g, there exists an isomorphism $\widetilde{\varphi} : K(a) \to L(b)$, in the sense that the following diagram commutes:*

(2.7)
$$\begin{array}{ccc} K(a) & \xrightarrow[\widetilde{\varphi}]{\cong} & L(b) \\ \uparrow & & \uparrow \\ K & \xrightarrow[\varphi]{\cong} & L. \end{array}$$

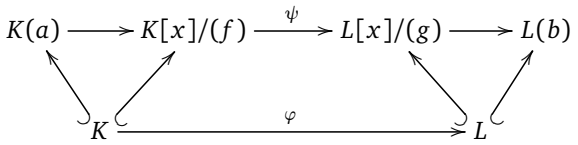
Proof. The isomorphism φ induces an isomorphism $K[x] \to L[x]$ defined by sending

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mapsto \varphi(a_n)x^n + \varphi(a_{n-1})x^{n-1} + \cdots + \varphi(a_1)x + \varphi(a_0),$$

and this maps f to g. Thus, it maps (f) to (g), so it defines an isomorphism $\psi : K[x]/(f) \to L[x]/(g)$. By Theorem 2.4, $K[x]/(f) \cong K(a)$ is an isomorphism of extensions of K, and similarly for $L[x]/(g) \cong L(b)$, so

[3] Finiteness is not necessary, but some sort of condition is needed: $k[x] \neq k(x)$ inside $k(x)$.

these isomorphisms fit together into the following commutative diagram of field homomorphisms, for which all horizontal arrows are isomorphisms.



Taking $\widetilde{\varphi}$ to be the composition across the top row reduces this diagram to (2.7) as desired. ⊠

Lecture III.

Finite Fields: Existence and Uniqueness

We already have examples of finite fields in the form of $\mathbb{F}_p$ for every prime p. In this section, we will characterize all finite fields, including an existence statement, a uniqueness statement, and a statement about when one finite field embeds in another.

Specifically, we will prove these statements.

Lemma 3.1. *If k is a finite field, then $|k| = p^n$, where p is prime and $n > 0$.*

Theorem 3.2. *For every prime p and $n > 0$, there exists a finite field of order p^n, and it is unique up to isomorphism over $\mathbb{F}_p$.*

This is why one often hears "*the* finite field of order p^n." Typically, this is denoted $\mathbb{F}_{p^n}$, or sometimes $\mathrm{GF}(p^n)$ in computer science.

Theorem 3.3. *Suppose $i : \mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{q^n}$ is an embedding. Then, $p = q$ and $m \mid n$. Conversely, if $m \mid n$, there is an embedding $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$.*

Together, these results classify all finite fields and their finite extensions.

Proof of Lemma 3.1. First, $\mathrm{char}(k) > 0$, because every characteristic 0 field contains a copy of $\mathbb{Q}$, which is infinite. Thus, there is a prime p such that $\mathrm{char}(k) = p$, so k is an extension of $\mathbb{F}_p$. Hence, k is an $\mathbb{F}_p$-vector space and a finite set, so it must be a finite-dimensional vector space. If $n = \dim_{\mathbb{F}_p} k$, then as abelian groups, $k \cong (\mathbb{F}_p)^n$, and in particular $|k| = p^n$. ⊠

We'll need two more ingredients, important in their own right, to tackle the existence and uniqueness questions.

Proposition 3.4. *If k is a field and $G \subseteq k^\times$ is a finite subgroup (so a finite group of nonzero elements of k, under multiplication), then G is cyclic. In particular, if k is a finite field, $k^\times$ is cyclic.*

Proof. Let's induct on the order of G; all groups of order at most 3 are cyclic, which is our base case.

Now, suppose G has order n. For any m, there are at most m elements of G of order dividing m, since such an $x \in G$ is a root of $x^m - 1 \in k[x]$, which has at most m roots.

If $n = p^\ell$ for some prime p, then G has at most $p^{\ell-1}$ elements of order dividing $p^{\ell-1}$. Thus, there's an $x \in G$ such that $|x| \nmid p^{\ell-1}$, but since $|G| = p^\ell$, then $|x| = p^\ell$, so $G = \langle x \rangle$ is cyclic.

The other option is for $n = ab$, where a and b are coprime. Since G is abelian, $f : x \mapsto x^a$ defines a group homomorphism $G \to G$; let $A = \ker(f)$ and $B = \mathrm{Im}(f)$. There are at most a elements of order dividing a, so $|A| \le a$. If $x \in B$, then $x = y^a$, and $x^b = y^{ab} = 1$, so $|x| \mid b$. There are at most b elements whose order divides b, so $|B| \le b$. By induction, A and B are cyclic, so if x generates A and y generates B, then $|x| = a$ and $|y| = b$, so $|xy| = ab = |G|$; thus, xy generates G, meaning G is cyclic. ⊠

Exercise 3.5. Show that if A is a commutative ring with $\mathrm{char}(A) = p$, then the assignment $\varphi : A \to A$ sending $x \mapsto x^p$ is a ring homomorphism. This φ is called the *Frobenius homomorphism* or *Frobenius endomorphism*; the corollary $(a+b)^p = a^p + b^p$ is also called the *freshman's dream*.

Proof of Theorem 3.2. First, we prove existence; then

⊠

Proof of Theorem 3.3. ⊠

Exercise 3.6. What is the underlying abelian group of the field $\mathbb{F}_{p^n}$?