(1) The main error was in some lack of rigor or clarity, so I'll just mention that the most common counterexample for power series was something like

$$(1-t)(1+t+t^2+t^3+\dots)=1$$

Notice that we can rewrite this as

$$\frac{1}{1-t}=\sum_{i-0}^{\infty}t^i$$

It's quite useful to take the usual Taylor series we know and just make them into formal power series. Often, many of the expected properties remain true in the formal setting. For example, we can define

$$\exp(t)=\sum_{n\geq 0}\frac{t^n}{n!}$$

and

$$\log(1+t)=\sum_{n\geq 1}\frac{(-1)^{n+1}t^n}{n}$$

Then one can compute $\exp(\log(1+t))=1+t$ as formal power series. I'll mention that composition of power series is subtle, and really only works when the inside function has no constant coefficient. This sort of thing is useful in algebra (and it's wonderful not thinking about convergence) for its ability to generalize these a priori real/complex analytic notion to many algebraic settings, such as the p-adics. It's also very useful in combinatorics via the theory of generating functions.

(2) Not many errors, so I'll say what I think are the cleanest methods.

$\boxed{char(F) \text{ is prime}}$ There is a unique map $\mathbb{Z}\longrightarrow F$. Its kernel is prime as F is a field. It cannot be (0) as F is finite, so it must be (p) for some prime p. Thus, $char(F)=p$.

$\boxed{|F|=p^n.}$ The above map induces an injective ring homomorphism $\mathbb{Z}/p\mathbb{Z}\longrightarrow F$, so we may view F as a module over $\mathbb{Z}/p\mathbb{Z}$. Thus, as $\mathbb{Z}/p\mathbb{Z}$ is a field, $F\cong(\mathbb{Z}/p\mathbb{Z})^n$ for some n as a $\mathbb{Z}/p\mathbb{Z}$ vector space. Thus, $|F|=p^n$.

$\boxed{\alpha^q=\alpha \text{ for } \alpha\in F.}$ Many people cited cyclicity of F^* here. This is the right idea, and is surely true, but we can get away without this somewhat difficult fact. Indeed, $|F^*|=q-1$ so by Lagrange's theorem, every element α of F has order dividing $q-1$. Hence, $\alpha^{q-1}=1$ for all nonzero α.

This is a priori weaker than saying F^* is cyclic of order $q-1$. Really, I used that the exponent of this finite abelian group (ie the smallest integer which kills every element) divides the order $q-1$. When the exponent equals the order, we have cyclicity, but we only need this divisibility.

(3) The main issue was not using the characteristic 0 hypothesis explicitly, which I discuss in (4) below.

(4) Many proofs used the fact that $\deg(f')=\deg(f)-1$ to deduce a contradiction since having a multiple root implies that $f|f'$. However, this uses that the characteristic of $\mathbb{C}$ is 0, which was often not mentioned. Here's a counterexample to the degree calculatiion in characteristic p.

Consider the field $F=\mathbb{F}_p(t)=qf(\mathbb{F}_p[t])$. Take the polynomial $f=x^p-t\in\mathbb{F}_p(t)[x]$. Then $f'(x)=px^{p-1}=0$ as the characteristic is p. Here, we do have $f|f'$ with no issues, as $f'=0$ and everything trivially divides 0.

The bizarre thing is that f has repeated roots in some extension field despite its irreducibility in this field. Indeed, let $K = F[x]/(f(x))$. This is a field extension of K in which f has a root. Let's call its root $t^{1/p}$ (Do you see why I'm calling it that? Is there any issue?), and remark that we would typically write $K = F(t^{1/p})$. Then in K we have the factorization $f(x) = (x - t^{1/p})^p$, by the Frobenius. Horrifying. This phenomenon is called "inseparability".

Another subtlety is not specifying in which field f and f' are coprime, i.e. in $F[x]$ or in $\mathbb{C}[x]$. To say something divides something else requires the context of a ring. This was a critical notion to 1900s number theorists, who realized the importance of understanding divisibility beyond the integers, which we have seen via our exploration of $\mathbb{Z}[i]$.

This is sheer pedantry, as I will show there is actually no difference. But it is important to resolve issues like this, as passing between fields is very subtle, as we shall see next quarter.

Lemma 0.1. *Let F be a subfield of a field K. Let $f, g \in F[x]$. Then f, g are coprime in $F[x]$ iff they are coprime in $K[x]$.*

Proof. We first show that if $f, g \in F[x]$ are coprime then they are coprime in $K[x]$. Indeed, by Bézout's identity we have $af + bg = 1$ for some $a, b \in F[x]$. But then this same equation holds in $K[x]$, so $(f, g) = (1)$ in $K[x]$ as well.

Now, suppose f, g are not coprime in $F[x]$. Then there is some nonzero nonunit $h \in F[x]$ so that $h|f$ and $h|g$ in $F[x]$. That is, $f = ah$ and $g = bh$ for $a, b \in F[x]$. These equations also hold in $K[x]$, so $h|f$ and $h|g$ in $K[x]$ whence f, g are not coprime in $K[x]$. □

In fact, more is true. The gcd of f and g will be the same in $F[x]$ and in $K[x]$. You can show this as the Euclidean algorithm will be the same for both fields (and, in fact, only cares about the field generated by the coefficients of f and g).

(5) The main error was in computing the dimension of $F[t]/(f)$. If $\deg(f) = n$, a basis for this space over F is $\overline{1}, \ldots, \overline{t^{n-1}}$. It spans $F[t]/(f)$ by the division algorithm. As for linear independence, suppose $\sum_{i=0}^{n-1} a_i \overline{t^i}$. Then $\overline{\sum_i a_i t^i} = 0$ so $f | \sum_i a_i t^i$. But $\deg(\sum a_i t^i) < n$ so this forces $\sum a_i t^i = 0$ whence all $a_i = 0$.

Additionally, in the second part about the $(\deg f)!$ bound, I think the best notation is as follows. Let $F_1 = F[t]/(f)$. Then f either splits in $F_1[t]$ or it has a nontrivial irreducible factor f_1. Let $F_2 = F_1[t]/(f_1)$. Iterate this process. The degrees of the polynomials being factored goes down, so the process terminates.

An interesting remark is that "most" polynomials over $\mathbb{Q}$ have splitting field of degree equal to $(\deg f)!$. The exact phrasing is a bit technical, but you can think of this as saying a random polynomial of degree n will with probability 1 have an $n!$ dimensional splitting field over $\mathbb{Q}$. This isn't rigorous, as I haven't told you the what probability means here. More formally, the set of tuples $(a_0, \ldots, a_n) \in \mathbb{Q}^{n+1}$ so that $\sum a_i t^i$ has splitting field of degree $n!$ is dense in the Zariski topology on $\mathbb{Q}^{n+1}$. We say that this set is Zariski dense. This means that there is no proper subvariety of $\mathbb{Q}^{n+1}$ which contains all the points with an $n!$ dimensional splitting field. This doesn't work over all fields, such as over finite fields where a degree n irreducible polynomial will have a splitting field of degree n.