

- (1) I don't have anything to say in terms of common errors. I'll say that the connection between irreducibility between $R[t]$ and $F[t]$ for R a UFD and F its quotient field is especially close when R is a local PID, also known as a discrete valuation ring (DVR). In that case, for a generator π of the maximal ideal of R , we can write every element of R as $u\pi^k$ for a unique unit $u \in R^*$ and $k \in \mathbb{N}$. So here, it's only powers of π (which is often called a uniformizer) in the denominator which could be a concern. Examples of DVRs include $\mathbb{Z}_{(p)}$, $\mathbb{Z}_p$, $k[t]_{(f)}$, and $k[[t]]$ where k is a field and f is an irreducible element of $k[t]$.

- (2) Not many errors here.

For one, this exact statement (and likely, your exact proof) is the same for any UFD replacing $\mathbb{Z}$.

Also one might notice that the hypotheses on a and b (being nonzero and coprime) are symmetric, so perhaps there is a hidden symmetry in this problem which swaps a and b so that we only have to prove one of the divisibilities. If so, swapping a and b would also have to swap a_0 and a_n .

Let $f = \sum_{i=0}^n a_i t^i$ with coefficients in some domain R . Suppose a_0 and a_n are nonzero. Let $g(t) = t^n f(1/t)$. Then $g \in R[t]$ and $g = \sum_{i=0}^n a_{n-i} t^i$. That is, we have swapped the order of the coefficients of f . Furthermore, the roots of g are precisely the reciprocals of the roots of f , including multiplicity. You can see this directly via the formula $g(t) = t^n f(1/t)$ or by applying Viète's formulas to $g(t) = \sum_{i=0}^n a_{n-i} t^i$ and to f itself.

The reciprocal of a/b is b/a , so $f(a/b) = 0$ iff $g(b/a) = 0$. Thus, only one divisibility needs to be proven. Of course, this is probably more work than just proving both divisibilities, but symmetry is always fun.

- (3) The biggest mistake was in conflating between elements of $F[t]$ and elements of $F[t]/(f)$. This is a reasonably common abuse of notation, but it is an abuse of notation and it's worth being cautious. For instance, it was common to write the nilradical as a subset of $F[t]$, but it has to be a subset of $F[t]/(f)$.

Another remark, somewhat along the same vein, is that I think it's best to write ideals of a quotient ring like $F[t]/(f)$ as $I/(f)$ for $(f) \subseteq I \subseteq F[t]$ an ideal. Such I exists and is unique by the correspondence principle. This is nice, for instance, as it allows computation with the third isomorphism quite easily. In this problem, if $f = \prod p_i^{e_i}$ where the p_i are distinct irreducibles, then $I = (\prod p_i)$. That is,

$$\text{nil}(F[t]/(f)) = \left(\prod p_i \right) / (f)$$

By the way, the unique $J \subseteq I \subseteq R$ for which $\text{nil}(R/J) = I/J$ is the *radical* of J , so $I = \sqrt{J}$. Here, we have

$$\sqrt{\left(\prod p_i^{e_i} \right)} = \left(\prod p_i \right)$$

This whole story works for any PID rather than just $F[t]$ or $\mathbb{Z}$. In fact, it works for $R/(f)$ for any UFD R and $f \in R$. Try the proof in this generality to ensure you see why the translation is so direct. When doing so, ensure you don't conflate elements of R and $R/(f)$, and try to write the final answer using the notation of the correspondence principle $I/(f)$.

- (4) Not many errors here.

I'll remark that it is exceedingly rare to understand all of the irreducible polynomials over a field. In this case, we have a uniform bound (of 2) on the degrees of irreducible polynomials. We have a uniform bound on degrees of irreducible polynomials over a field F if and only if F is algebraically closed, whence the bound is 1, or F is "real closed", whence the bound is 2.

A real closed field is one in which every element is a square or the negative of a square and so that all odd degree polynomials have roots. We can then justifiably call the nonzero squares *positive* and define an ordering on F . It turns out that F then satisfies the intermediate value theorem for polynomials, and more strongly is "elementarily equivalent" to $\mathbb{R}$ in the "language of ordered fields" which admits "quantifier elimination". I won't define any of these model theoretic terms, but essentially all real closed fields look like the reals in some sense. Another example of a real closed field are the real algebraic numbers, i.e. $\overline{\mathbb{Q}} \cap \mathbb{R}$.

For a real closed field F , we have the exact same characterization of irreducible polynomials as in this problem. This shows that $F[\sqrt{-1}]$ is algebraically closed, by the quadratic formula.

The statement that there is a uniform bound on degrees of irreducible polynomials over F is equivalent to saying that $\overline{F}/F$ is a finite degree extension of fields, where $\overline{F}$ is the algebraic closure of F . What I said above then means that, miraculously, $\overline{F}/F$ is finite iff F was already algebraically closed or F is real closed, in which case $\overline{F} = F[\sqrt{-1}]$. So somehow it never occurs that $\overline{F}/F$ is a degree 3 extension. This is all proven in Elman's book in the chapter on formally real fields. You can also read model theory books, such as Marker, for more on real closed fields.

(5) Not many errors here.

One thing I'll mention is that the same criterion holds for any domain R (so not a UFD) but you replace p with a prime ideal $\mathfrak{p}$, and the conclusion is that f cannot factor into nonconstant polynomials in $R[t]$. It's best used in UFDs, but it's still nice to have something in rings like $\mathbb{Z}[\sqrt{-5}]$.

Also, this is again especially useful in DVRs (see (1) above), as then you only have one prime to try. In "complete" DVRs (which I won't define) like $\mathbb{Z}_p$ and $k[[t]]$, this is especially powerful and has a generalization to Newton polygons, which are a very powerful computational tool when studying complete DVRs. These come up all the time in number theory to closely analyze how a prime p factors in some extension, as we did for $\mathbb{Q}(i)$, or in algebraic geometry to zoom in and locally understand a singularity of an algebraic curve.