

Partial Solutions to Homework 2

1. Stewart, exercise 1.7. This is a really long exercise. You should do it if you haven't done it in Math 113, but let's say it will not be graded.

(Besides 1.-5. on page 6, also show that \sim is an equivalence relation. Statement 2 just means that the result of addition and multiplication is indeed an element of F , i.e. that the second component of the result is non-zero.)

Only a few hints:

For proving that \sim is an equivalence relation, use that in an integral domain, $ab = bc$ implies $a = b$.

For statement 3, you have to prove that addition and multiplication are associative and commutative, that $[0, 1]$ is a zero element and that $[1, 1]$ is a unity element for the field, that $[p, q]$ has additive inverse $[-p, q]$ and multiplicative inverse $[q, p]$, and that the distributive laws hold.

For statement 4, check that the map is a homomorphism and determine its kernel.

2. Stewart, exercises 1.13 and 1.14.

(For 1.14, if $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with distinct prime numbers p_i and positive integers α_i , you should use the ring isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}$)

Solution:

For 1.13 see p.190. For 1.14 also see p. 190, you need to prove that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}$ has the required property if and only if each of the factors has the property. This is true since for the units of a product of rings with unity one has $(R \times S)^* = R^* \times S^*$. Now for $R = \mathbb{Z}_{p^\alpha}$, if $p > 3$, then 2 is a unit of order > 2 , since $2 \neq 1$ and $2^2 = 4 \neq 1$. The same holds if $p = 3$ and $\alpha > 1$. For $p = 2$ and $\alpha > 3$, 3 is a unit of order > 2 , since $3 \neq 1$ and $3^2 \neq 1$. Check that in the other cases R has the required property.

3. Let K be any field (think for example of \mathbb{Z}_p) and $f = \sum_{j=0}^n a_j t^j \in K[t]$. We define the **derivative** of f to be $Df = \sum_{j=1}^n k a_j t^{j-1}$. We get a map $D : K[t] \rightarrow K[t]$. (This is a purely algebraic map - we do not need analysis to define derivatives of polynomials.)

- Show that $D(f + g) = D(f) + D(g)$ and $D(fg) = D(f)g + fD(g)$ for $f, g \in K[t]$.
- Determine the kernel of D . (Attention!)
- Let $a \in K$, $f = (t - a)^n \cdot g$, where $g \in K[t]$ is s.t. $g(a) \neq 0$. Prove that $f(a) = (Df)(a) = (D^2 f)(a) = \cdots = (D^{n-1} f)(a) = 0$. For which fields K is $(D^n f)(a) \neq 0$?

Solution:

- should be routine.
- If the characteristic of K is p , then the kernel does not only consist of constant functions, but all polynomials of the form $a_{pn} t^{pn} + \cdots + a_p t^p + a_0$.
- Do induction on j to prove that

$$D^j f = n \cdot (n-1) \cdots (n-j+1)(t-a)^{n-j} g + (t-a)^{n-j+1} h$$

for $j \leq n$ and some polynomial h . The first statement follows immediately. And we see that $(D^n f)(a) \neq 0$ if and only if $n(n-1) \cdots 1 \neq 0$, i.e. if and only if the characteristic of K is 0 or $> n$.

4. Stewart, exercise 2.3.

Solution:

Prove that if $f(\alpha) = g(\alpha)$ for infinitely many $\alpha \in K$, then $f - g = 0$, since it has infinitely many zeros. If you restrict the degrees of f, g , you can have an even weaker assumption. In every case, use theorem 2.8.

5. Stewart, exercises 2.6 and 2.7.

Solution:

2.6 is a special case of 2.7. Let K be the field of characteristic $\neq 2$. Then $t^2 + at + b$ is irreducible if and only if the equation $x^2 + ax + b = 0 \Leftrightarrow (2x + a)^2 = a^2 - 4b$ has a solution $x \in K$. This is the case if and only if $a^2 - 4b$ is a square in K (which means that there is $c \in K$ s.t. $c^2 = a^2 - 4b$).