1. (DF9.4.8) Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2+1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2+2y+2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\overline{x})$ of K_1 to the element $p(\overline{y}+1)$ of K_2 (where p is any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.

   Proof. We show that the polynomials x^2+1 and y^2+2y+2 are irreducible in $\mathbb{F}_{11}[x]$ and $\mathbb{F}_{11}[y]$ respectively. Since both polynomials are quadratic, they are reducible if and only if they have linear factors; i.e., if they have roots in $\mathbb{F}_{11}$. Brute force calculation gives from which it follows that both polynomials cannot have

$\mathbb{F}_{11}$	x^2+1	y^2+2y+2
0	1	2
1	2	5
2	5	10
3	10	6
4	6	4
5	4	4
6	4	6
7	6	10
8	10	5
9	5	2
10	2	1

   linear factors and hence are irreducible. Since $\mathbb{F}_{11}$ is a field, it follows that $\mathbb{F}_{11}[x], \mathbb{F}_{11}[y]$ are Principal Ideal Domains. Thus x^2+1 and y^2+2y+2 are also prime elements so that the nonzero ideals (x^2+1) and (y^2+2y+2) are prime ideals, hence maximal ideals. It follows that K_1 and K_2 are indeed fields.

   We can find upper bounds for the number of elements each field has. Observe that in K_1 we have that $\overline{x}^2 = -1$, and in K_2 we have that $\overline{y}^2 = 2\overline{y}+2$. It follows that for any element of K_1 or K_2, its degree (where in K_1 and K_2 we can view the elements of these fields as polynomials in $\overline{x}$ or $\overline{y}$ respectively) is strictly less than 2, since any term with degree greater than or equal to 2 may be reduced in this manner (it may take many reductions to do so) into terms of degree 0 and 1.

   It follows that any element of K_1 takes the form $a\overline{x}+b$ and any element of K_2 takes the form $c\overline{y}+d$, where $a,b,c,d \in \mathbb{F}_{11}$. Since each of a,b,c,d can take on one of 11 values, it follows by counting that there are at most 121 elements of K_1 and the same for K_2. We can indeed exhibit all 121 elements of each field in exactly this manner:

$$K_1 = \{a\overline{x}+b \mid a,b \in \mathbb{F}_{11}\}$$

$$K_2 = \{c\overline{y}+d \mid c,d \in \mathbb{F}_{11}\}$$

   Let $\varphi\colon K_1 \to K_2$ be given by $p(\overline{x}) \mapsto p(\overline{y}+1)$; i.e., sending $\overline{x}$ to $\overline{y}+1$. We show that φ is well defined: Let r,s be polynomials with $\overline{r},\overline{s} = \overline{x}$. So $r = x + P(x)(x^2+1)^j$ and $s = x + Q(x)(x^2+1)^k$ for

polynomials P, Q and $k, j \geq 1$ (i.e. r and s project to $\overline{x}$). Then $\varphi(\overline{r}) = \overline{(y+1) + P(y+1)((y+1)^2+1)^j} = \overline{(y+1) + P(y+1)(y^2+2y+2)^j} = \overline{y} + 1$ and $\varphi(\overline{s}) = \overline{(y+1) + Q(x)((y+1)^2+1)^k} = \overline{y} + 1$ for the same reason. Hence $\overline{r}, \overline{s}$ map into the same equivalence class so φ is well defined.

We check that φ is a ring isomorphism:

For any elements $a(\overline{x}), b(\overline{x}) \in K_1$, we have that $\varphi(a(\overline{x}) + b(\overline{x})) = a(\overline{y}+1) + b(\overline{y}+1) = \varphi(a(\overline{x})) + \varphi(b(\overline{x}))$ and $\varphi(a(\overline{x})b(\overline{x})) = a(\overline{y}+1)b(\overline{y}+1) = \varphi(a(\overline{(x)}))\varphi(b(\overline{x}))$. Furthermore, the multiplicative identity in K_1 identity is the class 1, which is evidently mapped into the same class 1 in K_2. Thus φ is a ring (field) homomorphism. It suffices to show that this map is injective (since injective maps between sets of the same finite size are surjective), which we do using the trivial kernel characterization: Suppose some element $a(\overline{x})$ is mapped to the zero class in K_2; that is, $a(y+1)$ is divisible by $y^2 + 2y + 1$. This is equivalent to saying that $a(x)$ is divisible by $x^2 + 1$, since we can make the invertible change of variables $x \mapsto y + 1$ to obtain $x^2 + 1 \mapsto (y+1)^2 + 1 = y^2 + 2y + 2$. Hence $a(\overline{x})$ had to be the zero class in K_1, from which it follows that the kernel of φ is trivial and so φ is injective. Since both K_1, K_2 have the same finite size (121), it follows that φ is surjective also and hence bijective. Thus φ is a field isomorphism from K_1 to K_2. □

2. (DF9.4.15) Prove that if F is a field then the polynomial $X^n - x$ which has coefficients in the ring $F[[x]]$ of formal power series (cf. Exercise 3 of section 7.2) is irreducible over $F[[x]]$. [Recall that $F[[x]]$ is a Euclidean Domain — cf. Exercise 5, Section 7.2 and Example 4, Section 8.1.]

Proof. We apply Eisenstein's criterion to the polynomial $X^n - x$ in $(F[[x]])[X]$ directly. Observe that we can take the prime ideal $P = (x)$, which is prime since $F[[x]]/(x)$ is isomorphic to F, which is an integral domain (F is a field). Observe that $x \in P$, but $x \notin P^2 = (x^2)$. It follows that $X^n - x$ is irreducible in $(F[[x]])[X]$. □

3. (DF9.5.1) Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Describe the nilradical of $F[x]/(f(x))$ in terms of the factorization of $f(x)$ (cf. Exercise 29, Section 7.3).

Since F is a field, $F[x]$ is a Unique Factorization Domain, so that we can write $f(x)$ as a (unique up to associates) product of irreducible elements $p_i(x)$. In the case that $f(x)$ itself is irreducible (that is, if only one such $p_1(x)$ up to multiplication by a unit which constitutes the factorization of $f(x)$) then there are no nonzero nilpotent elements in $F[x]/(f(x))$ (every element which is nilpotent is of the form $g(x)p_1(x) + (f(x))$ for some $g(x) \in F[x]$, and $f(x)$ will divide the representative $g(x)p_1(x)$ so that the element is itself zero in the quotient ring) since $F[x]/(f(x))$ becomes a field.

Otherwise, we can factorize $f(x)$ into a nontrivial product of irreducibles $p_1^{e_1}(x) \cdots p_n^{e_1}(x)$ for some n and $e_i \geq 1$; here we adjust the choice of the irreducible factors since they are up to associates so that we can collect them into powers whenever possible. It follows that the nilradical of $F[x]/(f(x))$ is given by the set $\{g(x)p_1^{\alpha_1}(x) \cdots p_n^{\alpha_1}(x) + (f(x)) \mid g(x) \in F[x], \alpha_i \geq 1\}$; that is, the set of those cosets whose representative polynomial is divisible by every irreducible factor $p_i(x)$. Note that we could have used this formulation for

the case when $f(x)$ itself was irreducible, but we noted before that the set consists of only the zero class in $F[x]/(f(x))$.

These elements are indeed the nilpotent elements since we can always raise an element of the form $g(x)p_1^{\alpha_1}(x)\cdots p_n^{\alpha_1}(x)+(f(x))$ to a sufficiently large power k to ensure that each the resulting powers $k\alpha_i$ of each $p_i(x)$ exceed $\max\{e_i \mid 1\leq i\leq n\}$, in which case $f(x)$ divides the representative polynomial and so the element becomes the zero class in the quotient ring.

This is similar to our determination earlier in the case of the nilpotent elements of $\mathbb{Z}/n\mathbb{Z}$ where the nilpotent elements are those which are divisible by every prime factor of n. Here the nilpotent elements are those which are divisible by each of the irreducible (prime) factors of $f(x)$.

In these exercises R is a ring with 1 and M is a left R-module.

4. Auxiliary result for DF10.1.13: (DF10.1.7) Let $N_1\subseteq N_2\subseteq\cdots$ be an ascending chain of submodules of M. Prove that $M'=\cup_{i=1}^{\infty}N_i$ is a submodule of M.

   Proof. Every submodule N_i is nonempty subset of M so their union M' is also a nonempty subset of M. Let $x,y\in M'$, so that $x\in N_j$ and $y\in N_k$; without loss of generality suppose $k\geq j$ so that $x\in N_k$ also. By the submodule structure of N_k it follows that $x+ry\in N_k$ for all $r\in R$, and since x,y were arbitrary it follows that M' is a submodule of M. □

5. Auxiliary result for DF10.1.13: (DF10.1.10) If I is a right ideal of R, the *annihilator of I in M* is defined to be $M_1=\{m\in M \mid am=0 \text{ for all } a\in I\}$. Prove that the annihilator of I in M is a submodule of M.

   Proof. Observe that 0_M is annihilated by I due to the module structure on M ($r0_M=0_M$ for all $r\in R$), so that $0_M\in M_1$. It follows that M_1 is a nonempty subset of M, and let $x,y\in M_1$. Then for any $r\in R$, we have for any $a\in I$ that
   $$a(x+ry)=ax+a(ry)=0+(ar)y=0+0=0,$$
   with $ar\in I$ since I is a right ideal of R. Since x,y were arbitrary it follows that M_1 is a submodule of M. □

6. (DF10.1.13) Let I be an ideal of R. Let M' be the subset of elements a of M that are annihilated by some power I^k of the ideal I, where the power may depend on a. Prove that M' is a submodule of M. [Use Exercise 7.]

   Proof. Let M_k denote the annihilator of I^k in M, and recall that M_k are submodules of M. We show that $M_k\subseteq M_{k+1}$ for any $k\geq 1$: For any element $m_k\in M_k$, take any element $\sum_{i=1}^{n}a_{1i}a_{2i}\cdots a_{(k+1)i}$ of I^{k+1} and

see that

$$\begin{aligned}\left(\sum_{i=1}^{n} a_{1i}a_{2i}\cdots a_{(k+1)i}\right) m_k &= \sum_{i=1}^{n}(a_{1i}a_{2i}\cdots a_{(k+1)i})m_k \\ &= \sum_{i=1}^{n} a_{1i}[(a_{2i}\cdots a_{(k+1)i})m_k] \\ &= \sum_{i=1}^{n} a_{1i}0_M = 0_M,\end{aligned}$$

since each $(a_{2i}\cdots a_{(k+1)i})$ are elements of I^k. It follows that $m_k \in M_{k+1}$ and we obtain a chain $M_1 \subseteq M_2 \subseteq \cdots$ of submodules.

Observe that the union $M'' = \cup_{i=1}^{\infty} M_i$ is thus a submodule of M, and we show that $M' = M''$. It is clear that every element of M'' in M' since for any element $b \in M''$, we have that $b \in M_k$ for some k, meaning b is annihilated by I^k. Similarly, for any $a \in M'$, we have that a is annihilated by I^k for some k, meaning that $a \in M_k$. Thus $M' = M''$, meaning M' is a submodule of M. $\square$