

(1) Do exercise 15.24 in Judson

(a) $(f(x) + g(x))' = (\sum f_i x^i + \sum g_i x^i)' = (\sum (f_i + g_i) x^i)' = \sum (f_i + g_i) i x^{i-1} = \sum f_i i x^{i-1} + \sum g_i i x^{i-1} = f'(x) + g'(x)$

(b) If $f \in \ker(D)$, then $0 = f'(x) = \sum f_i i x^{i-1}$. So for each $i \in \mathbb{Z}^{\geq 0}$, $f_i i = 0$. Since F is an integral domain, one of these factors must be zero. Since F has characteristic zero, the only $i \in \mathbb{Z}^{\geq 0}$ which is zero in F is 0. Then for $i \neq 0$, $f_i = 0$. And f_0 can be anything. So the kernel is exactly the constant polynomials.

(c) If $f \in \ker(D)$, then $0 = f'(x) = \sum f_i i x^{i-1}$. So for each $i \in \mathbb{Z}^{\geq 0}$, $f_i i = 0$. Since F is an integral domain, one of these factors must be zero. Since F has characteristic p , $i \in \mathbb{Z}^{\geq 0}$ is only zero when $p \mid i$. Then for $p \nmid i$, $f_i = 0$. And when $p \mid i$, f_i can be anything. So the kernel of D is polynomials of the form $\sum f_{pj} x^{pj}$.

(d) $(f(x) \cdot g(x))' = ((\sum f_j x^j) \cdot (\sum g_k x^k))' = (\sum_i \sum_j f_j g_{j-i} x^i)' = \sum_i \sum_j i f_j g_{j-i} x^{i-1} = \sum_i \sum_j (j + (i - j)) f_j g_{j-i} x^{i-1} = \sum_i \sum_j j f_j g_{j-i} x^{i-1} + \sum_i \sum_j (i - j) f_j g_{j-i} x^{i-1} = (\sum j f_j x^{j-1}) \cdot (\sum g_k x^k) + (\sum f_j x^j) \cdot (\sum k g_k x^{k-1}) = f'(x)g(x) + f(x)g'(x)$

(e) Forward: We will prove the contrapositive. Suppose that $f(x)$ and $f'(x)$ were not relatively prime. Then they have some common divider $g(x)$ of degree at least 1. Since $g(x)$ divides $f(x)$ and is of positive degree, it must be divisible by $(x - a_i)$ for some i . Now $f(x) = (x - a_i) h(x)$ for some polynomial $h(x)$. By using part (d), we know $f'(x) = (x - a_i)' h(x) + (x - a_i) h'(x) = h(x) + (x - a_i) h'(x)$. Since $(x - a_i)$ divides $f'(x)$, it must divide $h(x)$. But then $(x - a_i)$ is a repeated factor of f .

Backward: Again we prove the contrapositive. Suppose $f(x)$ has a repeated factor $(x - a_i)$. Then $f(x) = (x - a_i)^2 h(x)$ for some $h(x)$. Now by (d), $f'(x) = ((x - a_i)^2)' h(x) + (x - a_i)^2 h'(x) = 2(x - a_i) h(x) + (x - a_i)^2 h'(x) = (x - a_i) (2h(x) + (x - a_i) h'(x))$. So both $f'(x)$ and $f(x)$ are divisible by $(x - a_i)$, so they are not relatively prime.

(2) Prove that $\mathbb{Z}[x]/\langle x^4 + 12 \rangle$ is an integral domain but not a field.

This is equivalent to showing that the ideal $\langle x^4 + 12 \rangle$ in $\mathbb{Z}[x]$ is prime but not maximal (in $\mathbb{Z}[x]$). To prove that $\langle x^4 + 12 \rangle$, assume that $a(x)b(x) \in \langle x^4 + 12 \rangle$ for some $a(x), b(x) \in \mathbb{Z}[x]$. So for some $c(x)$, $a(x)b(x) = c(x)(x^4 + 12)$. Note that since all these polynomials are in $\mathbb{Z}[x]$, they are in $\mathbb{Q}[x]$. Now If we apply Eisenstein's Criteria with $p = 3$, we get that $x^4 + 12$ is irreducible over \mathbb{Q} . Now the ideal generated by $x^4 + 12$ in $\mathbb{Q}[x]$ is maximal since \mathbb{Q} is a field and $x^4 + 12$ is irreducible. This ideal contains $a(x)b(x)$ and since it is maximal, it is prime. So either $a(x)$ or $b(x)$ is in the ideal generated by $x^4 + 12$ in $\mathbb{Q}[x]$. Without loss of generality, assume $a(x)$ is in, say $a(x) = d(x)(x^4 + 12)$ for some $d(x) \in \mathbb{Q}[x]$. By the proof of Gauss's Lemma $a(x) = (\alpha d(x))(\beta(x^4 + 12))$ where $(\alpha d(x)), (\beta(x^4 + 12)) \in \mathbb{Z}[x]$ and $\alpha, \beta \in \mathbb{Q}$. Now $\beta(x^4 + 12) = \beta x^4 + \beta 12$, so $\beta \in \mathbb{Z}$. Thus $\beta(\alpha d(x)) \in \mathbb{Z}[x]$, and so $a(x) \in \langle x^4 + 12 \rangle$ (the ideal is as computed in \mathbb{Z}).

Now to see that $\langle x^4 + 12 \rangle$, is not maximal in $\mathbb{Z}[x]$. Consider $I = 2\mathbb{Z}[x] + \langle x^4 + 12 \rangle = \{2f(x) + (x^4 + 12)g(x) : f(x), g(x) \in \mathbb{Z}[x]\}$. This is easily checked to be an ideal containing $\langle x^4 + 12 \rangle$. Since $2 \in I \setminus \langle x^4 + 12 \rangle$, we get $\langle x^4 + 12 \rangle \subsetneq I$. Also if 1 were in I , then $1 = 2f(x) + (x^4 + 12)g(x)$ for some $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$. If we consider this equation in $\mathbb{Z}_2[x]$, then $1 = x^4g(x)$, which is impossible since \mathbb{Z}_2 is a field. So $1 \notin I$, and $\langle x^4 + 12 \rangle \subsetneq I \subsetneq \mathbb{Z}[x]$. Thus $\langle x^4 + 12 \rangle$ is not maximal.

(3) Do exercise 19.1 in Judson

(a) $x^4 - \frac{2}{3}x^2 - \frac{62}{9}$

(b) $x^6 - 9x^4 - 10x^3 + 27x^2 - 90x - 2$

(c) $x^4 - 2x^2 - 25$

(d) Let $\omega = cis\frac{2\pi}{n}$. Then the minimal polynomial for ω is $\prod_{\substack{0 < k < n \\ \gcd(k,n)=1}} (x - \omega^k)$. Note

that this polynomial is always degree $\phi(n)$. For example, when $n = 6$, it is just $x^2 - x + 1$.

(e) $x^{12} + 3x^8 - 4x^6 + 3x^4 + 12x^2 + 5$

(4) Do exercise 19.5 in Judson

$x^3 + x + 1$ is irreducible because it has no roots and is degree three. By theorem 19.5, $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ has \mathbb{Z}_2 basis $\{1, x, x^2\}$. So the eight elements are $0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1$.

| | | | | | | | | |
|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| + | 0 | 1 | x | x+1 | x ² | x ² +1 | x ² +x | x ² +x+1 |
| 0 | 0 | 1 | x | x+1 | x ² | x ² +1 | x ² +x | x ² +x+1 |
| 1 | 1 | 0 | x+1 | x | x ² +1 | x ² | x ² +x+1 | x ² +x |
| x | x | x+1 | 0 | 1 | x ² +x | x ² +x+1 | x ² | x ² +1 |
| x+1 | x+1 | x | 1 | 0 | x ² +x+1 | x ² +x | x ² +1 | x ² |
| x ² | x ² | x ² +1 | x ² +x | x ² +x+1 | 0 | 1 | x | x+1 |
| x ² +1 | x ² +1 | x ² | x ² +x+1 | x ² +x | 1 | 0 | x+1 | x |
| x ² +x | x ² +x | x ² +x+1 | x ² | x ² +1 | x | x+1 | 0 | 1 |
| x ² +x+1 | x ² +x+1 | x ² +x | x ² +1 | x ² | x+1 | x | 1 | 0 |

| | | | | | | | | |
|---------------------|---|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| . | 0 | 1 | x | x+1 | x ² | x ² +1 | x ² +x | x ² +x+1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x+1 | x ² | x ² +1 | x ² +x | x ² +x+1 |
| x | 0 | x | x ² | x ² +x | x+1 | 1 | x ² +x+1 | x ² +1 |
| x+1 | 0 | x+1 | x ² +x | x ² +1 | x ² +x+1 | x ² | 1 | x |
| x ² | 0 | x ² | x+1 | x ² +x+1 | x ² +x | x | x ² +1 | 1 |
| x ² +1 | 0 | x ² +1 | 1 | x ² | x | x ² +x+1 | x+1 | x ² +x |
| x ² +x | 0 | x ² +x | x ² +x+1 | 1 | x ² +1 | x+1 | x | x ² |
| x ² +x+1 | 0 | x ² +x+1 | x ² +1 | x | 1 | x ² +x | x ² | x+1 |

(5) Do exercise 19.14 in Judson

Let $\alpha \in K$. Then α is algebraic over E , So for some $p(x) = p_nx^n + \dots + p_1x + p_0 \in E[x]$, $p(\alpha) = 0$. Now $p_n, \dots, p_0 \in E$, so they are each algebraic over F . So by Theorem 19.10, $[F(p_n, \dots, p_0) : F]$ is finite. Also, since $p(x) \in F(p_n, \dots, p_0)[x]$, $[F(p_n, \dots, p_0, \alpha) : F(p_n, \dots, p_0)]$ is finite. So $[F(p_n, \dots, p_0, \alpha) : F] = [F(p_n, \dots, p_0, \alpha) : F(p_n, \dots, p_0)] \cdot [F(p_n, \dots, p_0) : F]$ is also finite. So $F(p_n, \dots, p_0, \alpha)$ is an algebraic extension of F . In particular, α is algebraic over F . But α was an arbitrary element of K , so K is algebraic over F .

- (6) An automorphism of a field F is an isomorphism from F to itself. Prove that if f is an automorphism of $\mathbb{Q}(\sqrt{2})$, then for all $a, b \in \mathbb{Q}$, $f(a + b\sqrt{2}) = a \pm b\sqrt{2}$. Conclude that $\mathbb{Q}(\sqrt{2})$ has exactly two automorphisms.

Let f be an isomorphism of $\mathbb{Q}(\sqrt{2})$ to itself. Note that f is a group isomorphism from $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ to itself, so $f(1) = 1$. Now since $f(1 + 1 + \cdots + 1) = f(1) + f(1) + \cdots + f(1)$, so for $n \in \mathbb{Z}^+$, $f(n) = n$. Since $f(-n) = -f(n)$, f fixes \mathbb{Z} . And for $p \in \mathbb{Z}$ and $q \in \mathbb{Z}^{\neq 0}$, $f\left(\frac{p}{q}\right) = \frac{1}{f(q)}f(p) = \frac{1}{q}f(p) = \frac{1}{q} \cdot p = \frac{p}{q}$. So f fixes \mathbb{Q} . Now $f(\sqrt{2})^2 = f(\sqrt{2})f(\sqrt{2}) = f(\sqrt{2} \cdot \sqrt{2}) = f(2) = 2$. So $f(\sqrt{2}) = \pm\sqrt{2}$. So now $f(a + b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + b(\pm\sqrt{2})$ as desired.

- (7) Do exercise 19.26 in Judson

Consider $p(x) = x^2 - (\alpha + \beta)x + (\alpha\beta) = (x - \alpha)(x - \beta)$. By the first way of righting it, $p(x) \in \mathbb{Q}(\alpha + \beta, \alpha\beta)$. By the second way, we know $p(\alpha) = p(\beta) = 0$. So α and β are algebraic over $\mathbb{Q}(\alpha + \beta, \alpha\beta)$ and $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha + \beta, \alpha\beta)]$. Now if $\alpha\beta$ and $\alpha + \beta$ were algebraic over \mathbb{Q} , then $[\mathbb{Q}(\alpha + \beta, \alpha\beta) : \mathbb{Q}]$ would be finite. Then also $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha + \beta, \alpha\beta)] \cdot [\mathbb{Q}(\alpha + \beta, \alpha\beta) : \mathbb{Q}]$ would be finite. But α and β are transcendental. So at least one of $\alpha\beta$ and $\alpha + \beta$ must be transcendental as well.

- (8) Let $F \subset E$ be fields, and $a(x)$ and $b(x)$ are polynomials over F . Prove that $a(x)$ divides $b(x)$ in $E[x]$ if and only if $a(x)$ divides $b(x)$ in $F[x]$.

If $a(x)$ divides $b(x)$ in $F[x]$, then for some $c(x) \in F[x]$, $a(x)c(x) = b(x)$. But then $c(x) \in E[x]$, so $a(x)$ divides $b(x)$ there as well.

Now if $a(x)$ divides $b(x)$ in $E[x]$, then for some $c(x) \in E[x]$, $a(x)c(x) = b(x)$. We will prove that for all j , we have c_j in F . Suppose not. Let j be the minimum so that $c_j \notin F$. Let k be minimal so that $a_k \neq 0$. (If no such k exists, then $a(x) = b(x) = 0$ and 0 divides 0.) Now $b_{k+j} = \sum_{i=0}^{k+j} c_i a_{k+j-i} = \sum_{i=0}^j c_i a_{k+j-i}$. The second equality is if $i > j$, then $k + j - i < k$, so $a_{k+j-i} = 0$. Then $b_{k+j} = c_j a_i + \sum_{i=0}^{j-1} c_i a_{k+j-i}$. Since $a_i \neq 0$, we can solve for c_j :

$$c_j = \frac{1}{a_i} \left(b_{k+j} - \sum_{i=0}^{j-1} c_i a_{k+j-i} \right)$$

By assumption, $c_i \in F$ for $i < j$, so the righthand side is in F . So c_j is in F as well. Since $c_j \in F$ for all j , $c(x) \in F[X]$. So $a(x)$ divides $b(x)$ in $F[x]$.