Math 323 Homework 3

Problem 2 (Chapter 2.9)

> *Show that if D is a domain and F_1 and F_2 are fields such that D is a subring of each and each is generated by D, then there is a unique isomorphism of F_1 onto F_2 that is the identity map on D.*

Solution. Note that D commutative, since D is in a field: since $a, b \in D$, and so $a, b \in F$, and since F is a field, $ab = ba$.

Let $\eta_1 \colon D \to F_1$ be the identity homomorphism into F_1, which is a monomorphism since D is embedded in F_1 by definition of D generating F_1. Hence, if K is the field of fractions of D, we have that there is a unique monomorphism η_1' from K into F_1. The image of K in F_1 is a subring of F_1 that contains D, but by definition of D generating F_1, F_1 contains no proper subring that contains D, hence since η_1' must be surjective, so η_1' is a bijection. So there is a unique isomorphism of F_1 onto K. An identical argument also shows that there is a unique isomorphism of K onto F_2, by extending $\eta_2 \colon D \to F_2$ to $\eta_2' \colon K \to F_2$. Composing the two, namely $\eta_2' \circ \eta_1^{'-1}$, we get that there is a unique isomorphism from F_1 onto F_2.

Recall that η_1 and η_2 were the identity homomorphism of D, and so their extensions are also the identity map on D (and so too then also their inverses). Hence, the isomorphism $\eta_2' \circ \eta_1^{'-1}$ is the identity map on D.

Problem 5 (Chapter 2.9)

> *Let R be a commutative ring, and S a submonoid of the multiplicative monoid of R. In $R \times S$ define $(a, s) \sim (b, t)$ if there exists a $u \in S$ such that $u(at - bs) = 0$. Show that this is an equivalence relation in $R \times S$. Denote the equivalence class of (a, s) as a/s and the quotient set consisting of these classes as RS^{-1}. Show that RS^{-1} becomes a ring relative to*
>
> $$\begin{aligned} a/s + b/t &= (at + bs)/st \\ (a/s)(b/t) &= ab/st \\ 0 &= 0/1 \\ 1 &= 1/1 \end{aligned}$$
>
> *Show that $a \to a/1$ is a homomorphism of R into RS^{-1} and that this is a monomorphism if and only if no element of S is a zero divisor in R. Show that the elements $s/1$, $s \in S$, are units in RS^{-1}.*

Solution. We first show that $\sim$ is an equivalence relation. We have $(a, s) \sim (a, s)$, since for any $u \in S$, $u(as - as) = u \cdot 0 = 0$. For symmetry, assume that $(a, s) \sim (b, t)$. Then there is some $u \in S$ such that $u(at - bs) = 0$. Then $uat - ubs = 0 \implies 0 = ubs - uat = u(bs - at)$, so $(b, s) \sim (a, t)$. For transitivity, assume that $(a_1, s_1) \sim (a_2, s_2)$ and $(a_2, s_2) \sim (a_3, s_3)$. Then there exists $u_1, u_2 \in S$ such that $u_1(a_1 s_2 - a_2 s_1) = 0$ and $u_2(a_2 s_3 - a_3 s_2) = 0$. Hence $u_1 u_2 s_2(a_1 s_3 - a_3 s_1) = u_1 u_2 s_2 a_1 s_3 - u_1 u_2 s_2 a_3 s_1 - u_1 u_2 s_1 s_3 a_2 + u_1 u_2 s_1 s_3 a_2 = u_2 s_3 u_1(a_1 s_2 - a_2 s_1) + u_1 s_1 u_2(a_2 s_3 3 - a_3 s_2) = u_2 s_3 \cdot 0 + u_1 s_1 \cdot 0 = 0$, where we freely use the fact that R is a commutative ring and $u_1 u_2 s_2 \in S$. Thus, $(a_1, s_1) \sim (a_3, s_3)$, showing that $\sim$ is an equivalence relation.

We now prove that RS^{-1} is a ring. We first show that addition is well defined. Let $a/s \sim a'/s'$ and $b/t \sim b'/t'$, and so there exists $u_1, u_2 \in S$ such that $u_1(as' - a's) = 0$ and $u_2(bt' - b't) = 0$. We have the sums $(at + bs)/st$ and $(a't' + b's')/s't'$. Note $u_1 u_2((at + bs)s't' - (a't' + b's')st) = u_1 u_2((ats't' + bss't' - a't'st - b's'st) = u_2 u_1(as' - a's)tt' + u_1 u_2(bt' - b't)ss' = 0 + 0 = 0$, so $(at + bs)/st \sim (a't' + b's')/s't'$ and our sum is well-defined. Now we show $(RS^{-1}, +, 0)$ is an abelian group. We have $a/s + b/t = (at + bs)/st$ and $at + bs \in R$ and $st \in S$, so $a/s + b/t \in RS^{-1}$. For associativity, $(a/s + b/t) + c/u = (at + bs)/st + c/u = ((at + bs)u + cst)/stu = (atu + bsu + cst)/stu = (atu + (bu + ct)s)/stu = a/s + (b/t + c/u)$. For 0, $a/s + 0/1 = (a \cdot 1 + 0 \cdot s)/s \cdot 1 = a/s$ and $0/1 + a/s = (0 \cdot s + a \cdot 1)/1 \cdot s = a/s$. Also, $a/s + (-a)/s = (as - as)/ss = 0/s^2 \sim 0/1$ since for any $u \in S$ $u(0 \cdot 1 - 0 \cdot s^2) = u0 = 0$, and similarly, $(-a)/s + a/s \sim 0/1$. Finally, $a/s + b/t = (at + bs)/st = (bs + at)/ts = b/t + a/s$ since R is a commutative ring.

We now move on to multiplication. We first show that the multiplication is well-defined. Let $a/s \sim a'/s'$ and $b/t \sim b'/t'$, and $u_1, u_2 \in S$ as before. Actually, I'm just gonna skip verifying it is a ring because I'm running out of time.

Let $\phi\colon R \to RS^{-1}$ by $a \mapsto a/1$. Let $a, b \in R$. Then $\phi(a+b) = (a+b)/1 = a/1 + b/1 = \phi(a) + \phi(b)$. Also, $\phi(ab) = (ab)/1 = (a/1)(b/1) = \phi(a)\phi(b)$. Also, $\phi(1) = 1/1$ which is the multiplicative identity of RS^{-1}. So ϕ is a homomorphism.

Now assume that no element of S is a zero divisor in R. Let $a \in R$ such that $\phi(a) = a/1 \sim 0/1$. Then there is some $u \in S$ such that $u(a-0) = ua = 0$. We can't have $a \neq 0$, because then u is a zero divisor, which we assumed we didn't have, and so $a = 0$. Hence, $\ker\phi = \{0\}$, and so ϕ is a monomorphism.

Now assume that ϕ is a monomorphism. Then $\forall a \in R \setminus \{0\}$, $\phi(a) = a/1 \not\sim 0/1$, hence there is no $u \in S$ such that $ua = 0$, so S has no zero divisors.

Finally, consideer $s/1$, $s \in S$. Then $(s/1)(1/s) = s/s \sim 1/1$, and likewise, $(1/s)(s/1) \sim 1/1$, so $(s/1)^{-1} = 1/s \in RS^{-1}$. Thus, all $s/1$ are units.

Problem 2 (Chapter 2.10)

Show that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$ and that the real numbers $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent over $\mathbb{Q}$. Show that $u = \sqrt{2} + \sqrt{3}$ is algebraic and determine an ideal I such that $\mathbb{Q}[x]/I \cong \mathbb{Q}[u]$.

Solution. Assume there exists $a_0, a_1, \cdots \in \mathbb{Q}$ such that $\sqrt{3} = a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + a_3(\sqrt{2})^3 + \cdots$, which clearly is equivalent to there being $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$ (since each term is either an element in $\mathbb{Q}$, or an element in $\mathbb{Q}$ times $\sqrt{2}$). If we square both sides, we get $3 = a^2 + 2b^2 + 2ab\sqrt{2} \implies \sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ (since $\mathbb{Q}$ is a field), but by any standard proof, $\sqrt{2} \notin \mathbb{Q}$, a contradiction. Hence, there do not exist $a, b \in \mathbb{Q}$, and so $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

Recall from linear algebra it is sufficient to show, when $a_0, a_1, a_2, a_3 \in \mathbb{Q}$, that $a_0(1) + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} = 0$ only when $a_0 = a_1 = a_2 = a_3 = 0$. Note that our equation is equivalent to $(a_0 + a_1\sqrt{2}) + (a_2 + a_3\sqrt{2})\sqrt{3} = 0$. So we need only show that $\sqrt{3}, 1$ are linearly independent over $\mathbb{Q}[\sqrt{2}]$. But this is equivalent to saying that $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. So for the sake of contradiction, assume there is $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. Squaring both sides gives $3 = a^2 + 2ab\sqrt{2} + 2b^2 \implies \sqrt{2} = (3 - a^2 - 2b^2)2ab \in \mathbb{Q}$, but this is a contradiction. Hence, $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are linearly independent.

We want to show that there exists an $n \in \mathbb{N}^0$ and nonzero $a_i \in \mathbb{Q}$ such that $a_0 + a_1u + a_2u^2 + \cdots + a_nu^n = 0$. We have

$$1 - 10u^2 + u^4 = 1 - 50 - 20\sqrt{6} + 49 + 20\sqrt{6} = 0$$

Hence, $u = \sqrt{2} + \sqrt{3}$ is algebraic.

We want to find I such that $u = x + I$. I'm pretty sure this is $1 - 10x^2 + x^4$.

Problem 4 (Chapter 2.10)

Let $\Delta = \prod_{i>j}(x_i - x_j)$ in $\mathbb{Z}[x_1, \ldots, x_r]$ and let $\zeta(\pi)$ be the automorphism of $\mathbb{Z}[x_1, \ldots, x_r]$ which maps $x_i \to x_{\pi(i)}, 1 \leq i \leq r$. (Every automorphism of the ring $\mathbb{Z}[x_1, \ldots, x_r]$ is the identity on $\mathbb{Z}$. Why?) Verify that if τ is a transposition then $\Delta \to -\Delta$ under $\zeta(\tau)$. Use this to prove the result given in section 1.6 that if π is a product of an even number of transpositions, then every factorization of π as a product of transpositions contains an even number of transposititions. Show that $\Delta^2 \to \Delta^2$ under every $\zeta(\pi)$.

Solution. Let $\tau = (mn)$ be a transposition, where $1 \leq m, n \leq r$, $m \neq n$. Without loss of generality, let $n > m$. Since ζ is an automorphism, we have $\zeta(\tau)(\Delta) = \prod_{i>j}\zeta(\tau)(x_i - x_j) = \prod_{i>j}(x_{\tau(i)} - x_{\tau(j)})$. Consider each factor, $(x_{\tau(i)} - x_{\tau(j)})$. If $\tau(i) = i$ and $\tau(j) = j$, then $(x_{\tau(i)} - x_{\tau(j)}) = (x_i - x_j)$. If $\tau(i) = k$ and $\tau(j) = j$, we have that $(x_{\tau(i)} - x_{\tau(j)}) = (x_j - x_k)$, but we must have then $\tau(k) = i$ and there is some other factor $(x_{\tau(j)} - x_{\tau(k)}) = (x_j - x_i)$, and multiplication of polynomials is commutative, so we can swap these two terms and nothing changes. If $\tau(i) = j$ so $\tau(j) = i$, we have $(x_{\tau(j)} - x_{\tau(j)}) = (x_i - x_j) = -(x_j - x_i)$. This covers all the possible case in the product of Δ, and so, since there is only one factor that changes, specifically by picking up a negative, we have $\zeta(\tau)(\Delta) = -\Delta$. The result from 1.6 then follows, since we alternative negative signs.

Recall that every π can be decomposed as a product of transpositions. Hence, if $\pi = \tau_n\tau_{n-1}\cdots\tau_1$, we have $\zeta(\pi) = \zeta(\tau_n) \circ \zeta(\tau_{n-1}) \circ \cdots \circ \zeta(\tau_1)$. Since $\zeta(\pi)$ is an automorphism, we have $\zeta(\pi)(\Delta^2) = (\zeta(\pi)(\Delta))^2$. So

$$\zeta(\pi)(\Delta^2) = ((\zeta(\tau_n) \circ \zeta(\tau_{n-1}) \circ \cdots \zeta(\tau_1))(\Delta))^2 = (\pm\Delta)^2 = \Delta$$

where the second to last equality is from the fact $\zeta(\tau)(\Delta) = -\Delta$.

Problem 7 (Chapter 2.10)

> *Let $R[[x]]$ denote the set of unrestricted sequences $(a_0, a_1, \dots)$, $a_i \in R$. Show that one gets a ring from $R[[x]$ if one defines $+, \cdot, 0, 1$ as in the polynomial ring. This is called the ring of* formal power series in one indeterminate.

Solution. :)

Problem 1 (Chapter 2.11)

> *Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, $a_i \in F$, a field, $n > 0$ and let $u = x + (f(x))$ in $F[x]/(f(x))$. Show that every element of $F[u]$ can be written in one and only one way in the form $b_0 + b_1u + \cdots + b_{n-1}u^{n-1}$, $b_j \in F$.*

Solution. Let $c_0 + c_1u + \cdots + c_mu^m$ be an arbitrary element of $F[u]$. Since $F[u] \cong F[x]/(f(x))$, we have the isomorphism $\eta\colon F[u] \to F[x]/(f(x))$, where $c_0 + c_1u + \cdots + c_mu^m \mapsto c_0 + c_1x + \cdots c_mx^m + (f(x))$. By the division algorithm, there exists some $q(x), r(x) \in F[x]$, both unique since F is a field, such that

$$c_0 + c_1x + \cdots c_mx^m = q(x)f(x) + r(x)$$

where $\deg(r) < f(x)$. Since f has degree n, we can write $r(x) = b_0 + b_1x + \cdots + b_{n-1}u^{n-1}$, and so, since $q(x)f(x) \in (f(x))$,

$$c_0 + c_1x + \cdots c_mx^m + (f(x)) = b_0 + b_1x + \cdots + b_{n-1}u^{n-1} + (f(x))$$

Putting this back through η^{-1} (which we have because it is bijective) to $F[u]$, we get

$$\eta(c_0 + c_1x + \cdots c_mx^m) = \eta(b_0 + b_1x + \cdots + b_{n-1}u^{n-1})$$

and since η is injective, we have that

$$c_0 + c_1x + \cdots c_mx^m = b_0 + b_1x + \cdots + b_{n-1}u^{n-1}$$

and this is unique by the uniqueness of our remainder.

Problem 2 (Chapter 2.11)

> *Take $F = \mathbb{Q}$, $f(x) = x^3 + 3x - 2$ in exercise 1. Show that $F[u]$ is a field and express the elements*
>
> $$(2u^2 + u - 3)(3u^2 - 4u + 1), \qquad (u^2 - u + 4)^{-1}$$
>
> *as polynomials of degree ≤ 2 in u.*

Solution. To show that $F[u]$ is a field, by Theorem 2.16, it is sufficient to show that $f(x)$ is irreducible. For the sake of contradiction, assume that $f(x)$ is reducible. Then there exists $g(x), k(x) \in F[x]$ where $\deg(g), \deg(k) > 0$, such that $f(x) = g(x)k(x)$. Since $\deg(gk) = \deg(g) + \deg(k)$, we must have, assuming $\deg(g) \geq \deg(k)$, that $\deg(g) = 2$ and $\deg(k) = 1$. So $k(x)$ is of the form $k(x) = a_0 + a_1x$ where $a_0, a_1 \in \mathbb{Q}$. Hence, we have $f(-a_0/a_1) = (a_0 + a_1(-a_0/a_1))g(-a_0/a_1) = 0$. So $f(x)$ has a root at some rational. We'll let $\frac{p}{q} = -\frac{a_0}{a_1}$ where $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p, q) = 1$. So we have $0 = f(\frac{p}{q}) = p^3/q^3 + 3p/q - 2 = \frac{p^3 + 3pq^2 - 2q^3}{q^3} \implies p^3 + 3pq^2 - 2q^3 = 0$. Now consider this modulo q, then we have that $p^3 \equiv 0 \pmod q$, so p is a zero divisor in $\mathbb{Z}/(q)$. But from Theorem 2.4, since p and q are coprime, p is a unit in $\mathbb{Z}/(q)$. But an element cannot be both a unit and zero divisor in a ring, else $pp^2 = 0 \implies p^{-1}p^{-1}pp^2 = 0 \implies p = 0$, and 0 is not a unit, hence a contradiction. Thus, there is no linear polynomial factor of $g(x)$ in $\mathbb{Q}[x]$, and so $g(x)$ is irreducible. Thus $F[u]$ is a field.

Now, for $(2u^2 + u - 3)(3u^2 - 4u + 1)$, we can compute

$$(2u^2 + u - 3)(3u^2 - 4u + 1) = 6u^4 - 5u^3 - 11u^2 + 13u - 3$$

We can map this through the isomorphism η to $F[x]/I$ to get $6x^4 - 5x^3 - 11x^2 + 13x - 3 + I$. We can divide out by $f(x)$ to get an element in the same equivalence class:

$$6x^4 - 5x^3 - 11x^2 + 13x - 3 + I = (6x-5)(x^3+3x-2) + (-18x^2 + 27x - 10) + I = -18x^2 + 27x - 10 + I$$

Hence, putting this back through η^{-1} (which we have because it is bijective) to $F[u]$ we have

$$\eta((2u^2+u-3)(3u^2-4u+1)) = 6x^4 - 5x^3 - 11x^2 + 13x - 3 + I = -18x^2 + 27x - 10 + I = \eta(-18u^2 + 27u - 10)$$

And since η is injective, we have

$$(2u^2+u-3)(3u^2-4u+1) = -18u^2 + 27u - 10$$

For the second, we are looking for $g(u) = a_0 + a_1 u + a_2 u^2 \in F[u]$ such that $g(u)(u^2 - u + 4)$ (we need not check the other side because it is a field, and so commutative). We can compute

$$\begin{aligned} g(u)(u^2-u+4) &= a_0u^2 - a_0u + 4a_0 + a_1u^3 - a_1u^2 + 4a_1u + a_2u^4 - a_2u^3 + 4a_2u^2 \\ &= a_2u^4 + (a_1 - a_2)u^3 + (a_0 - a_1 + 4a_2)u^2 + (4a_1 - a_0)u + 4a_0 \end{aligned}$$

We can map this through the isomorphism η to $F[x]/I$ to get $a_2x^4 + (a_1-a_2)x^3 + (a_0 - a_1 + 4a_2)x^2 + (4a_1 - a_0)x + 4a_0 + I$. We can divide out by $f(x)$ to get an element in the same equivalence class:

$$\begin{aligned} &\big(a_2x^4 + (a_1-a_2)x^3 + (a_0-a_1+4a_2)x^2 + (4a_1-a_0)x + 4a_0\big) - (a_2x + (a_1-a_2))(x^3+3x-2) \\ =&(a_0-a_1+4a_2)x^2 + (4a_1-a_0)x + 4a_0 - 3a_2x^2 - 3(a_1-a_2)x + 2a_2x + 2(a_1-a_2) \\ =&(a_0-a_1+a_2)x^2 + (-a_0+a_1+3a_2)x + (4a_0 + 2a_1 - 2a_2) \end{aligned}$$

Hence, $a_2x^4 + (a_1-a_2)x^3 + (a_0-a_1+4a_2)x^2 + (4a_1-a_0)x + 4a_0 + I = (a_0 - a_1 + a_2)x^2 + (-a_0 + a_1 + 3a_2)x + (4a_0 + 2a_1 - 2a_2) + I$. If we want this to equal to $1 + I$, so we solve the system

$$\begin{cases} 0 = a_0 - a_1 + a_2 \\ 0 = -a_0 + a_1 + 3a_2 \\ 1 = 4a_0 + 2a_1 - 2a_2 \end{cases}$$

One can solve this system to find $a_0 = a_1 = \frac{1}{6}, a_2 = 0$. Given these assignments, then

$$a_2x^4 + (a_1-a_2)x^3 + (a_0-a_1+4a_2)x^2 + (4a_1-a_0)x + 4a_0 + I = 1 + I$$

Hence, if $g(u) = \frac{1}{6} + \frac{1}{6}u$, then $\eta(g(u)(u^2-u+4)) = 1 + I = \eta(1_{F[u]})$. Since η is a isomorphism, using injectivity, we get $g(u)(u^2-u+4) = 1_{F[u]}$, and so

$$(u^2-u+4)^{-1} = \frac{1}{6} + \frac{1}{6}u$$

Problem 3 (Chapter 2.11)

(a). *Show that $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt{3}]$ are not isomorhpic.*

(b). *Let $\mathbb{F}_p = \mathbb{Z}/(p)$, p a prime, and let $R_1 = \mathbb{F}_p[x]/(x^2-2)$, $R_2 = \mathbb{F}_p[x]/(x^2-3)$. Determine whether $R_1 \cong R_2$ in each of the cases in which $p = 2$, 5, or 11.*

(a). *Solution.* For the sake of contradiction, assume there exists some isomorphism $\phi\colon \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$. Note that any homomorphism between two fields that contain $\mathbb{Q}$ must be the identity map on itself: $\phi(1) = 1$ and so $\phi(1+1) = \phi(1) + \phi(1) = 2$. A simple induction would give us then $\phi(n) = n$ for all $n \in \mathbb{N}$. Then $0 = \phi(0) = \phi(n-n) = \phi(n) + \phi(-n) = n + \phi(-n) \implies \phi(-n) = -n$. So $\phi(n) = n$ for all $n \in \mathbb{Z}$. We also have $\phi(\frac{1}{n}) = \phi(n)^{-1} = n^{-1} = \frac{1}{n}$ for all $n \in \mathbb{Z}^*$, Hence, since each element in $\mathbb{Q}$ can be written as $\frac{m}{n}$ where $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we have $\phi(\frac{m}{n}) = \phi(m)\phi(\frac{1}{n}) = \frac{m}{n}$.

Since ϕ must be surjective, there exists some $q = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ such that $\phi(q) = \sqrt{3} \in \mathbb{Q}[\sqrt{3}]$. Thus,

$$3 = \phi(q)\phi(q) = \phi(q^2) = \phi(a^2 + 2ab\sqrt{2} + b^2) = a^2 + 2ab\phi(\sqrt{2}) + b^2$$

But then we have $\phi(\sqrt{2}) = \frac{3-a^2-b^2}{2ab} \in \mathbb{Q}$. Let this rational value be $q \in \mathbb{Q}$. So $\phi(\sqrt{2}) = q$. But we also have $q \in \mathbb{Q}[\sqrt{2}]$ and $\phi(q) = q$. And so $\phi(\sqrt{2}) = \phi(q)$. But since ϕ is an isomorphism, and so is injective, we have that $\sqrt{2} = q \implies \sqrt{2} \in \mathbb{Q}$, which is a contradiction.

(b). *Solution.* :)

Problem 4 (Chapter 2.11)

Show that x^3+x^2+1 is irreducible in $(\mathbb{Z}/(2))[x]$ and that $(\mathbb{Z}/(2))[x]/(x^3+x^2+1)$ is a field with eight elements.

Solution. For the sake of contradiction, assume that x^3+x^2+1 is reducible. Then there exists $g(x), k(x) \in (\mathbb{Z}/(2))[x]$ where $\deg(g), \deg(k) > 0$, such that $x^3+x^2+1 = g(x)k(x)$. Since $\deg(gk) = \deg(g)+\deg(k)$, we must have, assuming $\deg(g) \geq \deg(k)$, that $\deg(g) = 2$ and $\deg(k) = 1$. So $k(x)$ is of the form $k(x) = a_0 + a_1x$ where $a_0, a_1 \in \mathbb{Z}/(2)$. Since $a_1 \neq 0$, we must have $a_1 = 1$. Then either $k(x) = x$ or $k(x) = x+1$. Then either 0 or 1 is a root of x^3+x^2+1. But $0^3+0^2+1 = 1$ and $1^3+1^2+1 = 1$, so neither is a root, and so a contradiction. Hence, x^3+x^2+1 is irreducible.

Note that the ring $(\mathbb{Z}/(2))$ is a field: every nonzero element is a unit trivially $(= 1)$, and $0 \cdot 1 = 1 \cdot 0 = 1$ so its commutative. By theorem 2.6, any ideal of $(\mathbb{Z}/(2))/(x^3+x^2+1)$ is of the form $J/(x^3+x^2+1)$, where J is an ideal of $(\mathbb{Z}/(2))[x]$ containing (x^3+x^2+1). Since $(\mathbb{Z}/(2))[x]$ is a PID, we have that $J = (f(x))$. Since J contains (x^3+x^2+1), we have some $h(x)$ such that $x^3+x^2+1 = f(x)h(x)$. Since $g(x)$ is irreducible, either $\deg(f) = 0$ or $\deg(h) = 0$ (note $f(x) \neq 0 \neq h(x)$). So either $f(x) = 1$ or $h(x) = 1$. In the first case, $J = (\mathbb{Z}/(2))[x]$. In the second, $J = I$. So $(\mathbb{Z}/(2))[x]/(x^3+x^2 = 1)$ has only two ideals: 0 or the whole ring. Hence, by theorem 2.2, $(\mathbb{Z}/(2))[x]$ is a field.

We now show that $(\mathbb{Z}/(2))[x]/(x^3+x^2+1)$ has eight elements. Let $g(x)+(x^3+x^2+1)$ be an arbitrary element in $(\mathbb{Z}/(2))[x]/(x^3+x^2+1)$, specifically $g(x) = a_0 + a_1x + \cdots + a_mx^m \in (\mathbb{Z}/(2))[x]$. By the division algorithm, and the fact $(\mathbb{Z}/(2))[x]$ is a field, there exist unique $q(x), r(x) \in (\mathbb{Z}/(2))[x]$ such that $g(x) = q(x)(x^3+x^2+1)+r(x)$ and $\deg(r) < 3$. So $g(x)+(x^3+x^2+1) = r(x)+(x^3+x^2+1)$. So it is sufficient to characterize all of the elements of the form $r(x)+(x^3+x^2+1)$ where $r(x) \in (\mathbb{Z}/(2))[x]$ has at most degree 2. Note that there are 8 possible elements in $(\mathbb{Z}/(2))[x]$ with degree at most 2, namely $0, 1, x, x^2, 1+x, x+x^2, 1+x^2, 1+x+x^2$. Except for 0, none of these can be factored by x^3+x^2+1, since if $3 > \deg(r) > 0$, then there are no polynomials that can be multiplied with x^3+x^2+1 to have a product of $\deg(r)$, since $\deg(fg) = \deg(f)+\deg(g)$ in a field. Hence, all of these are distinct modulo (x^3+x^2+1). Thus, there are 8 distinct elements of $(\mathbb{Z}/(2))[x]/(x^3+x^2+1)$, corresponding to each $r(x)$ above.