oldfinala.pdf

1. (a) $a \in R$ is a unit if and only if there is a $b \in R$ such that $ab = 1_R$

   $a \in R$ is a zero divisor if and only if $a \neq 0_R$ adn there is a $b \in R$ such that $b \neq 0_R$ and $ab = 0_R$

   (If R is not commutative, we need to add more conditions: For unit: $ab = 1_R = ba$ For zero divisor: $ab = 0_R$ or $ba = 0_R$).

   (b) $R = \mathbb{Z}/(18) = \mathbb{Z}_{18}$. The units are those elements n such that $(n, 18) = 1$ (since this is the condition for the equation $nx = 1$ to have a solution in $\mathbb{Z}_{18}$). Then, $n = 1, 5, 7, 11, 13, 17$.

   (c) We need to solve $15x = 1$ in $\mathbb{Z}_{7564}$. We do the Euclidean algorithm,

   $$7564 = 15 \cdot 504 + 4$$

   $$15 = 4 \cdot 3 + 3$$

   $$4 = 3 \cdot 1 + 1$$

   $$3 = 1 \cdot 3$$

   Then $(7564, 15) = 1$, and there is a unique solution to the equation. To find it, we write 1 as a linear combination of 15 and 7564:

   $$1 = 4 - 3 = 4 - (15 - 4 \cdot 3) = 4 \cdot 4 - 15 = (7564 - 15 \cdot 504) \cdot 4 - 15 = 7564 \cdot 4 - 15 \cdot 2017$$

   Therefore, $15^{-1} = 2017$ in $\mathbb{Z}_{7564}$.

2. $f(x) = 5x^4 + 3x^3 + 1$, $g(x) = 3x^2 + 2x + 1$ in $\mathbb{Z}_7$. We apply the division algorithm dividing $5x^4 + 3x^3 + 1$ by $3x^2 + 2x + 1$:

   $$5x^4 + 3x^3 + 1 = (3x^2 + 2x + 1)4x^2 + (2x^3 + 3x^2 + 1),$$

   $$2x^3 + 3x^2 + 1 = (3x^2 + 2x + 1)3x + (4x^2 + 4x + 1),$$

   $$4x^2 + 4x + 1 = (3x^2 + 2x + 1)6 + (6x + 2).$$

   Therefore,

   $$5x^4 + 3x^3 + 1 = (3x^2 + 2x + 1)(4x^2 + 3x + 6) + (6x + 2).$$

   Now we divide $3x^2 + 2x + 1$ by $6x + 2$:

   $$3x^2 + 2x + 1 = (6x + 2)4x + (x + 1),$$

   $$x + 1 = (6x + 2)6 + 3.$$

   Therefore,

   $$3x^2 + 2x + 1 = (6x + 2)(4x + 6) + 3.$$

Finally, the Euclidean algorithm reads:

$$5x^4 + 3x^3 + 1 = (3x^2 + 2x + 1)(4x^2 + 3x + 6) + (6x + 2)$$

$$3x^2 + 2x + 1 = (6x + 2)(4x + 6) + 3$$

Then $(f(x), g(x)) = 1$. Furthermore, we have

$$3 = 3x^2 + 2x + 1 - (6x + 2)(4x + 6) = g(x) - (f(x) - g(x)(4x^2 + 3x + 6))(4x + 6)$$

$$= g(x)(1 + (4x^2 + 3x + 6)(4x + 6)) - f(x)(4x + 6) = g(x)(2x^3 + x^2 + 2) - f(x)(4x + 6)$$

We multiply by 5:

$$1 = g(x)(3x^3 + 5x^2 + 3) - f(x)(6x + 2)$$

3. (a) $2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2$ in $\mathbb{Q}[x]$. First we look for roots. Since $a_0 = 2$ and $a_5 = 2$, we try $r = -2$, and see that it is a root, since $-64 + 80 - 32 + 28 - 14 + 2 = 0$. Then we may write $2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 = (x + 2)(2x^4 + x^3 + 2x^2 + 3x + 1)$. We look at $2x^4 + x^3 + 2x^2 + 3x + 1$. Then $-\frac{1}{2}$ is a root, since $\frac{1}{8} - \frac{1}{8} + \frac{1}{2} - \frac{3}{2} + 1 = 0$. We write $2x^4 + x^3 + 2x^2 + 3x + 1 = (2x + 1)(x^3 + x + 1)$. Now $x^3 + x + 1$ does not have any roots in $\mathbb{Q}$, because the only possibilities are ± 1 (since $a_0 = a_3 = 1$) but $1 + 1 + 1 = 3$ and $-1 - 1 + 1 = -1$. Therefore, $x^3 + x + 1$ is irreducible, since a degree 3 polynomial without roots is irreducible. Therefore, the factorization in $\mathbb{Q}[x]$ is

$$2x^5 + 5x^4 + 4x^3 + 7x^2 + 7x + 2 = (x + 2)(2x + 1)(x^3 + x + 1).$$

(b) $x^3 + x^2 + x + 1$ in $\mathbb{Z}_2[x]$. It is easy to see that -1 is a root and $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$. But then 1 is also a root of $x^2 + 1$ and we obtain $x^2 + 1 = (x + 1)^2$. Finally, in $\mathbb{Z}_2[x]$,

$$x^3 + x^2 + x + 1 = (x + 1)^3.$$

(c) $x^{11} + 1$ in $\mathbb{Z}_{11}[x]$. Using the binomial expansion and the fact that $11 | \binom{11}{k}$ for any $1 \leq k \leq 10$, we get, in $\mathbb{Z}_{11}[x]$,

$$x^{11} + 1 = (x + 1)^{11}.$$

(We haven't covered this is class).

4. (a) A subring I of a commutative ring R is an ideal if for each $r \in R$ and $a \in I$ then $ra \in I$.

(b) $x \sim y \Leftrightarrow x - y \in A$. (i) We need to see that this is an equivalence relation. It is reflective: $x \sim x$ since $x - x = 0 \in A$ (since A is a subring). It is symmetric: $x \sim y$ implies $x - y \in A$ implies $y - x = -(x - y) \in A$ (since A is a subring) implies $y \sim x$. It is transitive: $x \sim y$ and $y \sim z$ imply that $x - y, y - z \in A$. Since A is a subring, $x - z = (x - y) + (y - z) \in A$, which implies $x \sim z$. (ii) $x \sim y$ and $u \sim v$ imply $x - y, u - v \in A$. Since A is a subring, $(x + u) - (y + v) = x - y + u - v \in A$ which implies that $x + u \sim y + v$. Also, since A is an ideal, $u(x - y), y(u - v) \in A$. Then $xu - yv = u(x - y) + y(u - v) \in A$, which implies $xu \sim yv$.

5. (a) We haven't see this.

   (b) (i) $5x^5+9x^4+15x^3+3x^2+6x+3$. We have that $p=3$ divides each of $a_0,\dots,a_4$, and it does not divide a_5. Further, $p^2=9$ does not divide a_0. By Eisenstein's criterion, the polynomial is irreducible.

   (ii) x^4+15x^3+7. We look at the polynomial in $\mathbb{Z}_2[x]$, we get x^4+x^3+1. This polynomial has no roots (check for $0,1$), and if it were the product of two degree 2 polynomials, it would be $(x^2+x+1)^2$ (since the others polynomials of degree 2 in $\mathbb{Z}_2[x]$ are reducible: x^2, $x^2+1=(x+1)^2$, $x^2+x=x(x+1)$). But $(x^2+x+1)^2=x^4+x^2+1\neq x^4+x^3+1$. Therefore the polynomial is irreducible.

   (c) We haven't seen this.

6. (a) It is well defined since $\phi(x)\in\mathbb{Z}_{12}$ for any $x\in\mathbb{Z}_3$.

   (b) $\phi(x+y)=4(x+y)=4x+4y=\phi(x)+\phi(y)$. $\phi(xy)=4(xy)=16xy=(4x)(4y)=\phi(x)\phi(y)$. We have used that $16=4$ in $\mathbb{Z}_{12}$.

   (c) $x\in\mathrm{Ker}(\phi)$ iff $\phi(x)=0$ iff $4x=0$ iff $3|x$ iff $x=0$ in $\mathbb{Z}_3$. Therefore $\mathrm{Ker}(\phi)=\{0\}$.

   (d) R^* is the set of units of R. In this case, $R^*=\{1,2\}$. No matter what we do, the image of ϕ is given by numbers that are "multiples" of 4 in $\mathbb{Z}_{12}$ and therefore they are not units. The answer is NO.

7. F field, and $A=\{f(x)\in F[x]\,|\,f(1)=0\}\subset F[x]$.

   (a) A is not empty, since $x-1\in A$.

   (b) Let $f(x),g(x)\in A$, then $f(1)=g(1)=0$. Now $(f-g)(1)=f(1)-g(1)=0$, which implies $f-g\in A$. If $f(x)\in A$ and $g(x)\in F[x]$, then $(fg)(1)=f(1)g(1)=0g(1)=0$. Therefore, $fg\in A$. Then A is an ideal.

   (c) Since $x-1\in A$, then $(x-1)F[x]\subset A$. We need to prove also that $A\subset(x-1)F[x]$. If $f\in A$, then $f(1)=0$, that means that 1 is a root of f. Therefore, $(x-1)|f(x)$ and we can write $f(x)=(x-1)g(x)$. But this shows that $f(x)\in(x-1)F[x]$ and $A\subset(x-1)F[x]$.

8. (a) The polynomials of degree 3 in $\mathbb{Z}_2[x]$ are $x^3, x^3+x^2, x^3+x, x^3+1, x^3+x^2+x, x^3+x^2+1, x^3+x+1, x^3+x^2+x+1$.

   (b) The maximal ideals are given by irreducible polynomials. We need to see which ones of the above polynomials are irreducible. Those whose constant coefficient is zero are clearly reducible (divisible by x). Then we just need to consider $x^3+1, x^3+x^2+1, x^3+x+1, x^3+x^2+x+1$. Those who have an even number of terms have $x=1$ as root. Then we need to look at x^3+x^2+1, x^3+x+1. Since neither 0 or 1 are roots, they must be irreducible, since degree 3 polynomials without roots are irreducible. The ideals are, therefore, (x^3+x^2+1) and (x^3+x+1).

   (c) Consider $\mathbb{Z}_5[x]/(f)$ where f is an irreducible polynomial of degree 2 in $\mathbb{Z}_5[x]$ (for example, it could be either x^2+2 or x^2+3, since they have no roots in $\mathbb{Z}_5[x]$). Then $\mathbb{Z}_5[x]/(f)$ is a field. It contains 25 elements, since all the elements may be written as $ax+b$ with 5 options for each coefficient.

oldfinalb.pdf

1. (1.1) We use the Euclidean algorithm:

$$726 = 275 \cdot 2 + 176$$

$$275 = 176 + 99$$

$$176 = 99 + 77$$

$$99 = 77 + 22$$

$$77 = 22 \cdot 3 + 11$$

$$22 = 11 \cdot 2$$

Therefore, $(726, 275) = 11$.

(1.2) From the above, $11 = 77 - 22 \cdot 3 = 77 - (99 - 77) \cdot 3 = 77 \cdot 4 - 99 \cdot 3 = (176 - 99) \cdot 4 - 99 \cdot 3 = 176 \cdot 4 - 99 \cdot 7 = 176 \cdot 4 - (275 - 176) \cdot 7 = 176 \cdot 11 - 275 \cdot 7 = (726 - 275 \cdot 2) \cdot 11 - 275 \cdot 7 = 726 \cdot 11 - 275 \cdot 29$. therefore,

$$11 = 726 \cdot 11 - 275 \cdot 29.$$

(1.3) Let $ua + vb, ra + sb \in A$. Then $(ua + vb) - (ra + sb) = (u - r)a + (v - s)b \in A$. Also, if $n \in Z$, then $n(ua + vb) = (nu)a + (nv)b \in A$. Therefore, A is an ideal.

(1.4) A is principal, it is in fact $A = (11)$. First, any combination of a and b is multiple of 11, therefore, $A \subset (11)$. On the other hand, 11 is a combination of a and b (see (1.2)), therefore, $11 \in A$, and $(11) \subset A$. So we get $(11) = A$.

2. (2.1) a, b, c nonzero integers. $(b, c) = d$, $(ab, c) = e$, and $(a, c) = 1$. Since any divisor of b is also a divisor of ab, we have that d is a common divisor for ab and c, and therefore $d|e$. Write $d = ub + vc$ for $u, v \in \mathbb{Z}$. Then $ad = uab + avc$ which implies that $e|ad$. Since $(a, c) = 1$, we can write $1 = xa + yc$. Now $d = xad + ycd$, and since $e|c$ and $e|ad$, we get $e|d$. Then $d|e$ and $e|d$ and they are positive (since they are gcds), implies that $e = d$.

(2.2) we haven't seen this.

3. We want to prove

$$n^2 + (n+1)^2 + \ldots + (2n)^2 = \frac{n(n+1)(14n+1)}{6}.$$

For $n = 1$, we have $1^2 + 2^2 = 5 = \frac{1 \cdot 2 \cdot 15}{6}$. Assume the result is true for $n = k$. Then for $n = k + 1$, we have

$$(k+1)^2 + \ldots + (2k+2)^2 = [k^2 + (k+1)^2 + \ldots + (2k)^2] + [(2k+1)^2 + (2k+2)^2 - k^2]$$

$$= \frac{k(k+1)(14k+1)}{6} + [(2k+1)^2 + (2k+2)^2 - k^2] = \frac{k(k+1)(14k+1)}{6} + (7k^2 + 12k + 5)$$

$$= \frac{k(k+1)(14k+1)}{6} + (k+1)(7k+5) = (k+1)\left[\frac{k(14k+1)}{6} + (7k+5)\right]$$

$$= (k+1)\left(\frac{14k^2 + 43k + 30}{6}\right) = \frac{(k+1)(k+2)(14k+15)}{6},$$

which proves the result.

4. Here $R = \mathbb{Z}_3$.

   (4.1) The elements of R are 0,1,2.

   (4.2) $2 + 2 = 1$ and $2^2 = 1$.

   (4.3) R is an integral domain since the products of nonzero elements are nonzero: $1 \cdot 1 = 1$, $1 \cdot 2 = 2$, $2 \cdot 1 = 2$ and $2 \cdot 2 = 1$.

   $S = R[x]/(x^2 + 1)$.

   (4.4) $0^2 + 1 = 1$, $1^2 + 1 = 2$ and $2^2 + 1 = 2$, so $x^2 + 1$ does not have roots in R.

   (4.5) A degree 2 polynomial without roots is irreducible.

   (4.6)$\alpha^2 = [x]^2 = -[1] = [2]$ in S.

   (4.7) S has 9 elements: $a\alpha + b$ where $a, b \in \{0, 1, 2\}$.

   (4.8) $\alpha^4 = [2]^2 = [1]$.

   (4.9) $\beta = [1] + \alpha$. Then $\beta^2 = ([1] + \alpha)^2 = [1] + 2\alpha + \alpha^2 = [1] + 2\alpha + [2] = 2\alpha$.

   (4.10) $\beta^8 = (2\alpha)^4 = [2]^4\alpha^4 = [16] = [1]$.

   (4.11) Since $x^2 + 1$ is irreducible in $R[x]$, then the quotient is a field, and non-zero elements in S are units.

oldfinalc.pdf

1. $7|(3^{2n} - 2^n)$:

   For $n = 1$, $7|(3^2 - 2^1) = 9 - 2 = 7$. Assume the statement is true for $n = k$. Now consider $n = k + 1$: $3^{2(k+1)} - 2^{k+1} = 9 \cdot 3^{2k} - 2 \cdot 2^k = 7 \cdot 3^{2k} + 2 \cdot 3^{2k} - 2 \cdot 2^k = 7 \cdot 3^{2k} + 2(3^{2k} - 2^k)$.

   Now the first term is divisible by 7 (since there is a 7 multiplying), and the second term is divisible by 7 by induction hypothesis. Therefore, $7 \cdot 3^{2k} + 2(3^{2k} - 2^k)$ is divisible by 7. This completes the induction.

2. (a) Let $[a], [b] \in S$, then $20|a$ and $20|b$. But then $20|(a + b)$ and therefore $[a + b] \in S$. For multiplication, $20|ab$ and therefore $[ab] \in S$. Clearly $[0] \in S$ by construction. Finally, the additive inverses are given by $-[0] = [0]$, $-[20] = [80]$, $-[40] = [60]$, $-[60] = [40]$, $-[80] = [20]$. Therefore S is a subring of $\mathbb{Z}_{100}$.

   (b) S is not an integral domain since $[20]^2 = [400] = [0]$ but $[20] \neq [0]$. It is not a field, since fields are integral domains.

   (c) $\mathbb{Z}_5$ is a field but S is not. Since being a unit is preserved by isomorphisms, then S can not be isomorphic to $\mathbb{Z}_5$.

3. (a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

are all idempotent.

(b) In $\mathbb{Z}_{12}$, $e^2 = e$ implies $e(e-1) = 0$. Therefore, $e = 0, 1$, or e is a zero divisor. The zero divisors are $2, 3, 4, 6, 8, 9, 10$. Of those, only 4 and 9 work. Thus, $e = 0, 1, 4, 9$.

(c) Since $e^2 = e$ implies $e(e-1) = 0$, we see that $e = 1$ or $e = 0$ solve the equation regardless of the ring.

(d) If we have an integral domain, there are no zero divisors, and therefore, the equation $e(e-1) = 0$ has only $e = 1$ or $e = 0$ as solutions.

4. (a) Let $f(t), g(t)$ be two polynomials in I_2. Then the coefficients of the polynomial $f(t) - g(t)$ are the difference of coefficients of $f(t)$ and $g(t)$, and therefore they have to be even. If $f(t) \in I_2$ and $g(t) \in \mathbb{Z}[t]$, then the product $f(t)g(t) \in I_2$. This is because if $f(t) = a_n t^n + \ldots a_0$ and $g(t) = b_m t^m + \ldots b_0$, then the product has coefficients that are sums of terms of the form $a_j b_{k-j}$ and each of those terms are even, since the a_i are even.

   (b) $I_2 = (2)$. Clearly the polynomial 2 is in I_2, and therefore $(2) \subset I_2$. On the other hand, any polynomial $f(t) \in I_2$ may be written as $f(t) = 2g(t)$ which shows that $f(t) \in (2)$.

   (c) This is the same as before. I_p is an ideal, and it is actually equal to (p).

5. (a) $f \sim g$ iff $t|(f-g)$. Then the following elements are equivalent to $3t^2 + 2t + 5$: $g(t) = 5, t + 5, t^2 + 5$. When we do the difference we get constant term zero, and therefore it is multiple of t.

   (b) Reflexive: $f \sim f$ since $t|(f-f) = 0$. Symmetric: $f \sim g$ implies that $t|(f-g)$, which implies that $t|(g-f)$, which implies that $g \sim f$. Finally, transitive: $f \sim g$ and $g \sim h$ imply that $t|(f-g)$ and $t|(g-h)$, but then $t|(f-g)+(g-h) = (f-h)$ which implies that $f \sim h$. Then we get an equivalence relation.

   (c) The elements that are equivalent to t are those whose constant coefficient is zero, i.e., f such that $f(0) = 0$.

6. (a) $T(9) = T(1+8) = T(1) + T(8) = T(1) + D = T(1) + T(4) = T(5) = A$.

   $T(10) = T(1+9) = T(1) + T(9) = T(1) + A = T(1) + T(1) = T(2) = B$.

   $T(11) = T(1+10) = T(1) + T(10) = T(1) + B = T(1) + T(2) = T(3) = C$.

   $T(12) = T(1+11) = T(1) + T(11) = T(1) + C = T(1) + T(3) = T(4) = D$.

   (b)

$+$	A	B	C	D
A	B	C	D	A
B	C	D	A	B
C	D	A	B	C
D	A	B	C	D

$+$	A	B	C	D
A	A	B	C	D
B	B	D	B	D
C	C	B	A	D
D	D	D	D	D

(c) The zero element is D, since the D row in the addition table is the same as the upper row.

(d) R is not an integral domain since $B^2 = D$, which is zero. It can not be a field, since any field is an integral domain.

7. $f(t) = 2t^4 + t^3 + t + 1$, $g(t) = t^3 + t^2 + 1$ in $\mathbb{Z}_3[t]$. We do the division algorithm

$$2t^4 + t^3 + t + 1 = (t^3 + t^2 + 1)2t + (2t^3 + 2t + 1)$$

$$2t^3 + 2t + 1 = (t^3 + t^2 + 1)2 + (t^2 + 2t + 2)$$

Therefore, the division algorithm reads

$$2t^4 + t^3 + t + 1 = (t^3 + t^2 + 1)(2t + 2) + (t^2 + 2t + 2).$$

Now we apply this again

$$t^3 + t^2 + 1 = (t^2 + 2t + 2)t + (2t^2 + t + 1)$$

$$2t^2 + t + 1 = (t^2 + 2t + 2)2$$

Therefore, the division algorithm reads

$$t^3 + t^2 + 1 = (t^2 + 2t + 2)(t + 2).$$

Therefore, $(f(t), g(t)) = t^2 + 2t + 2$.

We also get $t^2 + 2t + 2 = f(t) - g(t)(2t + 2) = f(t) + g(t)(t + 1)$.

8. Let $f(t) = \frac{1}{6}t^5 + \frac{2}{3}t^4 - \frac{1}{2}t^3 - 3t^2$. First of all, we can write $f(t) = \frac{1}{6}t^2\left(t^3 + 4t^2 - 3t - 18\right)$. We look for roots for the last factor. Let us try $t = 2$, since $2|18$. Then $8+16-6-18 = 0$. Therefore, we can write $f(t) = \frac{1}{6}t^2(t-2)(t^2+6t+9)$. Finally, it is easy to see (by the quadratic formula, for example), that $t^2 + 6t + 9 = (t + 3)^2$. Therefore,

$$f(t) = \frac{1}{6}t^2(t-2)(t+3)^2.$$

9. (a) $p(t) = 21t^3 - 6t + 8$. We reduce to $\mathbb{Z}_5$: $p(t) = t^3 - t + 3$. We look for roots: $p(0) = 3$, $p(1) = 3$, $p(2) = 4$, $p(3) = 2$, $p(4) = 3$. Then there are no roots in $\mathbb{Z}_5$ and the polynomial is irreducible since its degree is 3. Therefore, there are no roots in the rationals as well.

(b) $q(t) = 3t^{10} + 5f(t)$ with deg $f(t) < 10$ and $f(0) = 17$.

(i) We could take, for example, $q(t) = 3t^{10} + 5 \cdot 17$.

(ii) Take $p = 5$. Then p divides the coefficients, except for the principal one. Also, $f(0) = 17$ implies that the constant coefficient of f is 17 and the constant coefficient of q is $17 \cdot 5$. Therefore p^2 does not divide the constant coefficient of q. By Eisenstein criterion, q is irreducible

10. $p(t) = t^4 + t^2 + 1$.

(a) Notice that $t^4 + t^2 + 1 = (t^2 + t + 1)^2$, therefore p is not irreducible and $\bar{R}$ is not a field.

(b) $[t^3+t^2+1]_{p(t)}+x = [t^2+t]_{p(t)}$ implies $x = [t^2+t]_{p(t)}-[t^3+t^2+1]_{p(t)} = [t^3+t+1]_{p(t)}$. The answer is uniquely determined since addition inverses are unique.

(c) $[t^3 + t^2 + 1]_{p(t)}x = [t^2 + t]_{p(t)}$. First we find the multiplicative inverse for $[t^3 + t^2 + 1]_{p(t)}$. For that, we need $a, b \in \mathbb{Z}_2[t]$ such that $a(t^3 + t^2 + 1) + bp(t) = 1$. We do euclidean algorithm:

$$t^4 + t^2 + 1 = (t^3 + t^2 + 1)t + (t^3 + t^2 + t + 1)$$

$$t^3 + t^2 + t + 1 = (t^3 + t^2 + 1) + t$$

then the division algorithm is

$$t^4 + t^2 + 1 = (t^3 + t^2 + 1)(t + 1) + t.$$

One more time,

$$t^3 + t^2 + 1 = t(t^2 + t) + 1.$$

Then $1 = (t^3+t^2+1)+t(t^2+t) = (t^3+t^2+1)+((t^4+t^2+1)+(t^3+t^2+1)(t+1))(t^2+t) = (t^3 + t^2 + 1)(t^3 + t + 1) + (t^4 + t^2 + 1)(t^2 + t)$. Therefore, the inverse of $[t^3 + t^2 + 1]_{p(t)}$ is given by $[t^3 + t + 1]_{p(t)}$. Now

$$x = [t^3+t^2+1]^{-1}_{p(t)}[t^2+t]_{p(t)} = [t^3+t+1]_{p(t)}[t^2+t]_{p(t)} = [t^5+t^4+t^3+t]_{p(t)} = [(t^3+t)+(t^2+1)+t^3+t]_{p(t)}$$

$$= [t^2 + 1]_{p(t)}.$$