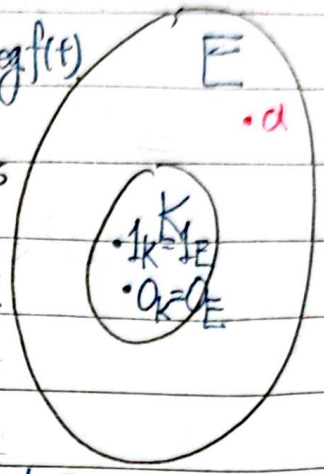
Date / /

2024/11/25 MATH3301 Tutorial 11

1(a) Solution: Assume to the contrary that $\deg g(t) < \deg f(t)$



As both $f(t)$ and $g(t)$ are nonzero polynomials in $K[t]$, where K is a field, we can apply the Division Algorithm to find:

(1) The monic greatest common divisor $h(t) \neq 0$ of $f(t), g(t)$ in $K[t]$;

(2) At least a pair of polynomials $\lambda(t), \mu(t)$ in $K[t]$, such that $\lambda(t)f(t) + \mu(t)g(t) = h(t)$

We wish to show that $h(t)$ is not a constant. If so, then $f(t)$ has a nonconstant proper factor $h(t)$ ($0 < \deg h(t) < \deg f(t)$), contradicting to $f(t)$ is irreducible in $K[t]$.

To see this, regard the following equation in $K[t]$ as an equation in $E[t]$ as $K[t] \leq E[t]$:

$$\lambda(t)f(t) + \mu(t)g(t) = h(t).$$

Evaluate both sides at $t = \alpha$, and we get $h_E(\alpha) = \lambda(\alpha)0 + \mu(\alpha)0 = 0$.

Hence, the monic polynomial $h(t)$ is not a constant, and we're done.

To solve the equation $\lambda(t)f(t) + \mu(t)g(t) = h(t)$ in $K[t]$, one may reduce $f(t)$ to $q(t)g(t) + r(t)$, $\deg r(t) < \deg g(t)$, and solve the easier one:

$$\lambda'(t)r(t) + \mu'(t)g(t) = h(t)$$

$\lambda'(t) = \lambda(t)$, $\mu'(t) = \mu(t) + \lambda(t)q(t)$

Date / /

(b) Proof: We may divide our proof into two parts.

"$\subseteq$" inclusion: For all $h(t) \in K[t]$:

$$h(t) \in \langle f(t) \rangle \Rightarrow \exists\, \lambda(t) \in K[t],\ h(t) = \lambda(t) f(t)$$

$$\Rightarrow h_E(\alpha) = \lambda_E(\alpha) 0 = 0$$

$$\Rightarrow h(t) \in \{g(t) \in K[t] : g_E(\alpha) = 0\}$$

"$\supseteq$" inclusion: Assume to the contrary that some $h(t)$ $\in \{g(t) \in K[t] : g_E(\alpha) = 0\}$ is not in $\langle f(t) \rangle$.

As $f(t), h(t)$ are polynomials in $K[t]$ with $f(t) \neq 0$, where K is a field, we can apply the Division Algorithm to find a unique pair of polynomials $q(t), r(t)$ in $K[t]$, such that $h(t) = q(t)f(t) + r(t)$, $\deg r(t) < \deg f(t)$.

Evaluate both sides at $t = \alpha \in E$, we get $r_E(\alpha) = 0 - q(\alpha)0 = 0$

Hence, $r(t) \in \{g(t) \in K[t] : g_E(\alpha) = 0\}$ and $-\infty < \deg r(t) < \deg f(t)$.

Contradicting to (a).

To conclude, we've proven that $\langle f(t) \rangle = \{g(t) \in K[t] : g_E(\alpha) = 0\}$.

2.(a) i. Solution: Assume that P is a nonzero prime ideal of R.

For all $y \in P^c$, we wish to prove that $\langle y \rangle + P = R$.

As the prime ideal P contains $0 = y^{2015} + y = y(y^{2014}+1)$, P contains at least one of $y, y^{2014}+1$, so $y \notin P$ implies $y^{2014}+1 \in P$

Assume that $x = y^{2014}+1 \in P$, notice that:

(1) $(-y^{2013}) \in R$ and $y \in \langle y \rangle$, so $(-y^{2013})y \in \langle y \rangle$;

(2) $x \in P \subseteq P + \langle y \rangle$ and $(-y^{2013})y \in \langle y \rangle \subseteq P + \langle y \rangle$,

so $1 = x + (-y^{2013})y \in P + \langle y \rangle$,

and we've shown that $P + \langle y \rangle = R$, i.e., P is maximal.

ii. Solution: $R[t]/\langle t^2+t+1 \rangle$ is not a field.

As $|R| = 49 = 7^2$, where 7 is prime, it follows from Theorem 12.3.3 that $Char(R) = 7$, so for all integers $n, m \in \mathbb{Z}$, $[n = m \text{ in } R] \Leftrightarrow [n \equiv m \pmod 7 \text{ in } \mathbb{Z}]$.

As $Deg(t^2+t+1) = 2 > Deg(t-2) = 1 > -\infty$,

t^2+t+1 doesn't divide $t-2$, $t-2 \notin \langle t^2+t+1 \rangle$, $t-2$ is not a unit.

As $(t-2)(t-4) = t^2 - 6t + 8 = t^2 + (7-6)t + (7+1) = t^2+t+1$ in $R[t]$, $t-2$ divides t^2+t+1, $\langle t^2+t+1 \rangle \subsetneq \langle t-2 \rangle \subsetneq R[t]$.

As for some ideal $\langle t-2 \rangle$ of $R[t]$, $\langle t^2+t+1 \rangle \subsetneq \langle t-2 \rangle \subsetneq R[t]$ and $\langle t^2+t+1 \rangle \neq R[t]$, $\langle t^2+t+1 \rangle$ is not maximal in $R[t]$, so it follows from Proposition 10.2.2. that $R[t]/\langle t^2+t+1 \rangle$ is not a field.

(b) Solution: Theorem 12.3.3. suggests that the finite field $F(2015<|F|<2200)$ has order p^n, where $p \geq 2$ is a prime number, and $n \geq 1$ is an integer.

This p is the characteristic of F, i.e., the smallest k in $\mathbb{Z}_{>0}$ such that $k=0$ in F. As some r in $\mathbb{Z}_{>0}$ satisfies $r<20$ and $r=0$ in R, it must be true that:

$$p \leq r \leq 19, \quad p \in \{2,3,5,7,11,13,17,19\}$$

Case 1: $p=2$. Now $2=0$ in R, contradicting to:

$$0 = 5 \cdot 0 = 5 \cdot 2 = 10 \neq 0 \text{ in } R.$$

Case 2: $p=3$. Now $3=0$ in R, and the following sequence implies that n must be 7:

$$3^1=3<3^2=9<3^3=27<3^4=81<3^5=243$$

$$<3^6=729<2015<3^7=2187<2200<3^8=6561$$

$\leq$ every 3^n with $n \geq 8$.

In this case, $10 = 3 \cdot 3 + 1 = 3 \cdot 0 + 1 = 0 + 1 = 1 \neq 0$ in R, and $12 = 4 \cdot 3 = 4 \cdot 0 = 0$ in R for some $12<20$ in $\mathbb{Z}$.

Case 3: $p=5$. Now $5=0$ in R, contradicting to:

$$0 = 2 \cdot 0 = 2 \cdot 5 = 10 \neq 0 \text{ in } R.$$

Case 4: $p=7$. Now $7=0$ in R, and the following sequence implies that $n \in \emptyset$, so this case is impossible:

$$7^1=7<7^2=49<7^3=343<2015<2200<7^4=2401$$

$\leq$ every 7^n with $n \geq 4$.

Date / /

Case 5: $p=11$. Now $11=0$ in R, and the following sequence implies that $n \in \emptyset$, so this case is impossible:

$$11^1=11<11^2=121<11^3=1331<2015<2200<11^4=14641 \leq \text{every } 11^n \text{ with } n \geq 4.$$

Case 6: $p=13$. Now $13=0$ in R, and the following sequence implies that n must be 3:

$$13^1=13<13^2=169<2015<13^3=2197<2200<13^4=28561 \leq \text{every } 13^n \text{ with } n \geq 4.$$

In this case $2<10<13$, so $10 \neq 0$ in R, and $13=0$ in R for some $13<20$ in $\mathbb{Z}$.

Case 7: $p=17$. Now $17=0$ in R, and the following sequence implies that $n \in \emptyset$, so this case is impossible:

$$17^1=17<17^2=289<2015<2020<17^3=4913 \leq \text{every } 17^n \text{ with } n \geq 3.$$

Case 8: $p=19$. Now $19=0$ in R, and the following sequence implies that $n \in \emptyset$, so this case is impossible:

$$19^1=19<19^2=361<2015<2020<19^3=6859 \leq \text{every } 19^n \text{ with } n \geq 3.$$

To conclude, $(\text{Char}(F), |F|)=(3, 3^7=2187)$ or $(13, 13^3=2197)$

If $\text{Char}(F)=3$, then $t^2-3=t^2=t \cdot t$ for some nonconstant polynomials $t, t \in F[t]$. This implies t^2-3 is reducible in $F[t]$.

If $\text{Char}(F)=13$, then $t^2-3=t^2-16=(t+4)(t-4)$ for some nonconstant polynomials $t+4, t-4 \in F[t]$. This implies t^2-3 is reducible in $F[t]$.

Date

3. (a) Solution: $t^2+t+1=(t+\frac{1}{2})^2+\frac{3}{4}$ is a second order polynomial in $\mathbb{R}[t]$.

It has no root in $\mathbb{R}[t]$, so it is irreducible in $\mathbb{R}[t]$.

It follows from Theorem 11.2.16. that $\mathbb{R}[t]/\langle t^2+t+1\rangle$ is a field.

t^2+t+1 is a second order polynomial in $\mathbb{F}_{13}[t]$.

As $\mathrm{Deg}(t^2+t+1)=2>\mathrm{Deg}(t-3)=1>-\infty$,

t^2+t+1 doesn't divide $t-3$, $t-3\notin\langle t^2+t+1\rangle$, $t-3$ is not a unit.

As $(t-3)(t-9)=t^2-12t+27=t^2+(13-12)t+(2\cdot 13+1)=t^2+t+1$

in $\mathbb{F}_{13}[t]$, $t-3$ divides t^2+t+1, $\langle t^2+t+1\rangle\subsetneq\langle t-3\rangle\subsetneq\mathbb{F}_{13}[t]$ and

$\langle t^2+t+1\rangle\neq\mathbb{F}_{13}[t]$, $\langle t^2+t+1\rangle$ is not maximal in $\mathbb{F}_{13}[t]$, so it follows

from Proposition 10.2.2. that $\mathbb{F}_{13}[t]/\langle t^2+t+1\rangle$ is not a field.

(b) Solution: $(\bar{t}^2+1)^1=(-\bar{t})^1=\bar{t}+1$ in $\mathbb{Z}_2[t]/\langle t^2+t+1\rangle$.

$(\bar{t}^2+1)^2=(-\bar{t})^2=\bar{t}^2=-\bar{t}-1=\bar{t}+1\neq 1$ in $\mathbb{Z}_2[t]/\langle t^2+t+1\rangle$.

$(\bar{t}^2+1)^3=(-\bar{t})^3=\bar{t}^2\bar{t}=(\bar{t}+1)\bar{t}=\bar{t}^2+\bar{t}=\bar{t}+1+\bar{t}=1$ in $\mathbb{Z}_2[t]/\langle t^2+t+1\rangle$

Hence, $\mathrm{Ord}(\bar{t}^2+1)=3$.

As $|(\mathbb{Z}_2[t]/\langle t^2+t+1\rangle)^\times|=3$, $\bar{t}^2+1$ is actually a generator.

4. (a) Solution: The following table shows that the second order polynomial $f(t)=t^2+2t+3$ has no root in $\mathbb{Z}_5[t]$, thus irreducible:

The congruence class of t_0	The evaluation of t_0^2+2t+3
0	3
1	$6\equiv 1$
2	$11\equiv 1$
3	$18\equiv 3$
4	$27\equiv 2$

It follows from Theorem 11.2.16. that $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$ is a field.

Date

$(4\bar{t}+1)^1 = 4\bar{t}+1$ in $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$

$(4\bar{t}+1)^2 = 16\bar{t}^2+8\bar{t}+1 = -32\bar{t}-48+8\bar{t}+1$

$= -24\bar{t}-47 = \bar{t}+3$ in $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$

$(4\bar{t}+1)^3 = (\bar{t}+3)(4\bar{t}+1) = 4\bar{t}^2+13\bar{t}+3$

$= -8\bar{t}-12+13\bar{t}+3 = 5\bar{t}-9 = 1$ in $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$

Hence, $Ord(4\bar{t}+1)=3$.

(b) Solution: This is impossible.

Assume to the contrary that a ring homomorphism $\phi: \mathbb{Z}_5[t]/\langle t^2+2t+3\rangle \to \mathbb{Z}_{25}$ exists. Now ϕ(The unity 1 of $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$) = The unity 1 of $\mathbb{Z}_{25}$. This implies:

The zero in $\mathbb{Z}_{25}$ = ϕ(The zero in $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$)

= ϕ(The five in $\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$) (Char($\mathbb{Z}_5[t]/\langle t^2+2t+3\rangle$)=5)

= The five in $\mathbb{Z}_{25}$

This is a contradiction because $Char(\mathbb{Z}_{25}) = 25 > 5$.

Hence, no such ring homomorphism exists.

5.(a) Solution:

$\bar{t}^1 = \bar{t}$ in $\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle$

$\bar{t}^2 = -4\bar{t}-1 = \bar{t}+4$ in $(\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle)^\times$

$\bar{t}^3 = \bar{t}^2+4\bar{t} = -1$ in $(\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle)^\times$

It follows that $Ord(\bar{t})=6$ in $(\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle)^\times$

If we multiply $\bar{t}$ by $\bar{t}+2$, where $Ord(\bar{t}+2)=8$

then we get a generator $\bar{t}^2+2\bar{t} = 3\bar{t}+4$ of $(\mathbb{Z}_5[t]/\langle t^2+4t+1\rangle)^\times$

because $l.c.m(6,8)=24$

Date / /

(b) Solution: As it is possible to complete square in $\mathbb{F}_p[t]$:

$$at^2+bt+c\,(c\neq 0)=a\left(t+\frac{b}{2a}\right)^2+\left(c-\frac{b^2}{4a}\right)$$

It suffices to prove that every $a\in\mathbb{F}_p$ has at least one square root in $\mathbb{F}_{p^2}$.

Case 1: If a already has a square root r in $\mathbb{F}_p$, then we are done because $\mathbb{F}_p$ can be embedded in $\mathbb{F}_{p^2}$ by natural projection $s\mapsto s$.

Case 2: If a has no square root in $\mathbb{F}_p$,

then choose $b\in\mathbb{F}_p$, such that b^2-a has no square root in $\mathbb{F}_p$.

This $b\in\mathbb{F}_p$ always exists, let's prove by contradiction.

Assume to the contrary that such b fails to exist.

That is, for all $b\in\mathbb{F}_p$, b^2-a has a square root $b_1\in\mathbb{F}_p$

Now $b^2-2a=b_1^2-a$ has a square root $b_2\in\mathbb{F}_p$,

$b^2-3a=b_1^2-2a=b_2^2-a$ has a square root $b_3\in\mathbb{F}_p$,

$\vdots$ $\quad\vdots$ $\quad\vdots$

$b^2-ka=\cdots=b_{k-1}^2-a$ has a square root $b_k\in\mathbb{F}_p$.

As $a\neq 0$ has no square root, it follows that $a=b^2-\left(\frac{b^2-a}{a}\right)a$ has a square root, contradiction!

Now define an imaginary unit $w=\sqrt{b^2-a}$, and extend the field $\mathbb{F}_p$ to a larger field $\mathbb{F}_p[w]$.

It suffices to notice that $(b+w)^{\frac{p+1}{2}}$ is a square root of a in $\mathbb{F}_p[w]$:

$$\left[(b+w)^{\frac{p+1}{2}}\right]^2=(b+w)(b+w)^p=(b+w)\sum_{k=0}^{p}\binom{p}{k}b^{p-k}w^k$$

$$=(b+w)(b^p+w^p)=(b+w)(b-w)=b^2-w^2=a.$$

Here, $b^p=b$ follows from Fermat's Little Theorem in $\mathbb{F}_p$.

and $w^p=w\in\mathbb{F}_p[w]^\times$ as $|\mathbb{F}_p[w]^\times|=p^2-1$. As x^p-x cannot have more than p roots, $w^p=-w$

6. Proof: We would like to show that $R^\times$ has an element of order 8.

Assume to the contrary that $R^\times$ has no element of order 8. According to the classification theorem for finite Abelian groups, $R^\times \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$ or $R^\times \cong (\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_3$. Now every element in [2-part] satisfies $x^4 = 1$, contradicting to $x^4 - 1$ has at most 4 roots (as assumed).

Hence, $R^\times \cong \mathbb{Z}_6 \times \mathbb{Z}_3 \cong \mathbb{Z}_{2^k}$ is cyclic.