Algebra Endsem

Somnath Bhattacharjee
BMC201954

May 31, 2021

Question 1.

We can say any homomorphism from $\mathbb{Z}[x]$ to $\mathbb{R}$ or $\mathbb{C}$ has a kernel Principal ideal
Since we can regard that homomorphism in $\mathbb{Q}[x]$ and here the kernel is principal as $\mathbb{Q}[x]$ is PID
Now Let that ideal be I, clearly $J = \mathbb{Z}[x] \cap I$ is the kernel of the initial map
Now Let $cf_0(x)$ is the generator of I where f_0 is primitive
Now if we kill the denominator of c we can say it will generate J in $\mathbb{Z}[x]$

We know that homomorphism from $\mathbb{Q} \to \mathbb{C}$ is unique
(as let $\phi : \mathbb{Q} \to \mathbb{C}$ be a homomorphism
Now $\phi\big|_{\mathbb{Z}}$ is unique, now for $n \in \mathbb{Z}$ we can say $\phi(\frac{1}{n}) = \phi(n)^{-1}$ which is unique , hence ϕ is unique as $\phi(\frac{p}{q}) = \phi(p)\phi(q)^{-1}$ for $p, q \in \mathbb{Z}, q \neq 0, (p,q) = 1$)

We can actually generalise this fact to any arbittrary ring, if there exists at all any homomorphism then that must be unique

Hence the only homomorphism from $\mathbb{Q} \to \mathbb{C}$ is the inclusion

Now from substitution principle we can have an unique injective homomorphism from $\mathbb{Q}[x] \to \mathbb{C}$ for $x \to z$ for $z \in \mathbb{C}$, z is transcendental over $\mathbb{Q}$ ....(i)
(it will be injective because inclusion is injective now $\phi(p(x)) \neq 0$ since $\phi(x)$ is transcendental over $\mathbb{Q}$
Now we will prove a claim

Claim. Any injective homomorphism from $\phi : \mathbb{Q}[x] \to \mathbb{C}$, where $x \to z$, $z \in \mathbb{C}$, can be extended to a unique homomorphism $\tilde{\phi}$ from $\mathbb{Q}(x) \to \mathbb{C}$ where $\tilde{\phi}\big|_{\mathbb{Q}[x]} = \phi$ and vice versa

Let ϕ be such homomorphism
Define $\tilde{\phi} : \mathbb{Q}(x) \to \mathbb{C}$

$$\tilde{\phi}\big|_{\mathbb{Q}[x]} = \phi$$

for $p(x) \in \mathbb{Q}[x]$ with degree ≥ 1

$$\tilde{\phi}(p(x)^{-1}) = \phi(p(x))^{-1}$$

(as $\mathbb{C}$ is a field we know the 'inverse' exists as $p(x) \neq 0$, hence $\phi(p(x)) \neq 0$ as ϕ injective)
Now from the universal property of fraction field of a domain we can say $\tilde{\phi}$ is well defined and works well and is unique

For the converse part assume $\tilde{\phi} : \mathbb{Q}(x) \to \mathbb{C}$ be a homomorphism
Now since $\mathbb{Q}(x)$ is afield we can sa the kernel must be 0 or $\mathbb{Q}(x)$, now $\mathbb{Q}(X)$ can not be the kernel since 1 must map with 1, hence the map is injective
Now we can take the restricted map $\phi = \tilde{\phi}|_{\mathbb{Q}[x]}$and from the uniqueness part in the substitution principle we are done

Now from (i) and the previous claim we can say all possible homomorphism from $\mathbb{Q}(x)$ to $\mathbb{C}$ are actuaclly extended version of all possible homomorphism $\phi : \mathbb{Q}[x] \to \mathbb{C}$ which sends $x \to z$ where z is transcendental over $\mathbb{Q}$

Now we can generalise that calculation to any arbitrary ring R, if there exists any homomophism at all then it must sends $x \to$ a transcendental element over $\mathbb{Q}$ and its restriction on $\mathbb{Q}$ is the unique homomorphism from $\mathbb{Q}$

Question 2.

i. $r = 201954 = 2 \times 3 \times 97 \times 347$
Now $2 = (1+i)(1-i)$
3 is a gauss prime
$97 = (9+i4)(9-4i)$
347 is a gauss prime as $347 \equiv 3 \mod 4$
Now Let σ be the size function
Now $\sigma(7+4i) = 65$ which can be written as 13×5
Now observe $13 = (2+3i)(2-3i)$ and $5 = (1+2i)(-1+2i)$
Hence we can write $7+4i = (1+2i)(-1+2i)(2+3i)(2-3i)$
Hence $7r + 4ri = r(1+2i)(-1+2i)(2+3i)(2-3i) = 3 \times 347(1+i)(1-i)(9+i4)(9-4i)(1+2i)(-1+2i)(2+3i)(2-3i)$
Since $\mathbb{Z}[i]$ is UFD is we got our factorisation

ii. we can factorise $p'(x) = 320x^5 - 2430 = 10(2x-3)(16x^4 + 24x^3 + 36x^2 + 54x + 81)$ normally
(we did it because of a nice observation that $p'(\frac{3}{2}) = 0$, and then long division)

Claim. $p(x) = 16x^4 + 24x^3 + 36x^2 + 54x + 81$ is irreducible over $\mathbb{Z}[x]$

we know that $p(x)$ is irreducible in $\mathbb{Q}[x]$ iff so is $p(\frac{x}{2})$
Now $p(\frac{x}{2}) = x^4 + 3x^3 + 9x^2 + 27x + 81$
Now in $\mathbb{F}_2[x]$ $p(\frac{x}{2})$ is equivalent to $q(x) = x^4 + x^3 + x^2 + x + 1$
Now $q(\bar{1}) = 1 = q(\bar{0})$
Hence q has no root in $\mathbb{F}_2$
Hence $q(x)$ can not have any degree one or degree 3 monic irreducible factor in $\mathbb{F}_2[x]$ Now suppose q has a degree 2 irreducible monic factor in $\mathbb{F}_2[x]$ then it must

be (x^2+x+1) since it is the only one degree 2 monic irreducible polynomial in $\mathbb{F}_2[x]$
Hence $q(x) = (x^2+x+1)^2 = x^4+1$ which is not possible
Hence $q(x)$ is irreducible in $\mathbb{F}_2[x]$
Hence $p(x/2)$ is irreducible in $\mathbb{Q}[x]$ and hence so is $p(x)$
Now GCD of $16, 24, 36, 54, 81$ is 1 hence $p(x)$ is primitive
Hence $p(x)$ irreducible over $\mathbb{Z}[x]$
Hence our claim is true

Now $p'(x) = 2 \times 5 \times (2x-3) \times (16x^4 + 24x^3 + 36x^2 + 54x + 81)$ and each of the factors are irreducible in $\mathbb{Z}[x]$ and $\mathbb{Z}[x]$ is UFD
Hence we got our desired factorisation

iii. again we can factorise $p(x) = x^4 - r^2x^2 + x - r = (x-r)(x^3 + rx^2 + 1)$
Now if $q(x) = x^3 + rx^2 + 1$ is reducible in $\mathbb{Q}[x]$ then it must have an irreducible one degree polynomial element as a factor hence a root in $\mathbb{Q}$
It is clear that $q(0), q(1), q(-1) \neq 0$
Now suppose $\frac{p}{q}$, $p, q \in \mathbb{Z} - 0, (p,q) = 1$ is a root of $q(x)$
then

$$q(\frac{p}{q}) = 0 = \frac{p^3}{q^3} + r^2\frac{p^2}{q^2} + 1$$

or,

$$q \big| p^3 + rp^2q + q^3 \text{ and } p \big| p^3 + rp^2q + q^3$$

or,

$$q \big| p \text{ and } p \big| q$$

Hence $|p| = |q| = 1$ as $(p,q) = 1$
or, $\frac{p}{q} = 1$ or -1
which contradicts that $q(1) \neq$ or $q(-1) \neq 0$
Hence $q(x)$ has no roots in $\mathbb{Q}$
Hence q is irreducible in $\mathbb{Q}[x]$

Now GCD of $1, r^2, 1$ is 1
Hence $q(x)$ is primitive
Hence it is irreducible in $\mathbb{Z}[x]$
As $\mathbb{Z}[x]$ is UFD the factorisation is $p(x) = (x-r)(x^3 + rx^2 + 1)$

Question 3.

i. For any homomorphism $\mathbb{Z}[x] \to \mathbb{R}$ we know the kernel will be a principle ideal
Now since $\mathbb{R}$ is a domain , any subring of that will be a domain hence $\mathbb{Z}[x]/kernel$ will be a domain, hence the kernel will be prime, hence the generator of that ideal will be irreducible

Now suppose there is a homomorphism $\phi : \frac{\mathbb{Z}[x]}{\langle x^4 + rx^2 \rangle} \to \mathbb{R}$ then we will have a homomorphism $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{R}$ with $\langle x^4 + rx^2 \rangle \subseteq$ the kernel and vice-versa

Now if we have a homomorphism $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{R}$ with $\langle x^4 + rx^2 \rangle \subseteq$ the kernel then the ideal will be generated by one of irreducible factor of $x^4 + rx^2$

Now $x^4 + rx^2 = x^2(x^2 + r)$

Now $r = 201954$ is divisible by 2 but not by 4, hence $x^2 + r$ is irreducible in $\mathbb{Q}[x]$, also it is primitive hence irreducible in $\mathbb{Z}[x]$
Hence either $\langle x \rangle$ or $\langle x^2 + r \rangle$ is the kernel
Now $\tilde{\phi}(r) = r > 0$ and $\tilde{\phi}(x^2) = \tilde{\phi}^2(x) \geq 0$ as it is in $\mathbb{R}$
Hence $\tilde{\phi}(x^2 + r) \neq 0$
Hence the only possibility is x
Hence there is only one homomorphism from $\frac{\mathbb{Z}[x]}{\langle x^4+rx^2 \rangle} \to \mathbb{R}$ is that which sends $\overline{x}$ to 0 and k to k for $k \in \mathbb{Z}$

We will go with the similar way to the previous part
For any homomorphism $\mathbb{Z}[x] \to \mathbb{C}$ we know the kernel will be a principle ideal
Now since $\mathbb{C}$ is a domain , any subring of that will be a domain hence $\mathbb{Z}[x]/kernel$ will be a domain, hence the kernel will be prime, hence the generator of that ideal will be irreducible

Now suppose there is a homomorphism $\phi : \frac{\mathbb{Z}[x]}{\langle x^4+rx^2 \rangle} \to \mathbb{C}$ then we will have a homomorphism $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{C}$ with $\langle x^4 + rx^2 \rangle \subseteq$ the kernel and vice-versa

Now if we have a homomorphism $\tilde{\phi} : \mathbb{Z}[x] \to \mathbb{C}$ with $\langle x^4 + rx^2 \rangle \subseteq$ the kernel then the ideal will be generated by one of irreducible factor of $x^4 + rx^2$

Now $x^4 + rx^2 = x^2(x^2 + r)$
Now $r = 201954$ is divisible by 2 but not by 4, hence $x^2 + r$ is irreducible in $\mathbb{Q}[x]$, also it is primitive hence irreducible in $\mathbb{Z}[x]$
Hence either $\langle x \rangle$ or $\langle x^2 + r \rangle$ is the kernel
Now if $\tilde{\phi}(x) = 0$ then the map will be 3 which sends $\overline{x}$ to 0 and $k \to k$ for $k \in \mathbb{Z}$

Now if $\tilde{\phi}(x^2 + r) = 0$ then $\tilde{\phi}^2(x) = \pm i\sqrt{r}$
Hence we have two maps from $\frac{\mathbb{Z}[x]}{\langle x^4+rx^2 \rangle}$ to $\mathbb{C}$, one sends $\overline{x}$ to $i\sqrt{r}$ and $k \to k$ for $k \in \mathbb{Z}$ another sends $\overline{x}$ to $-i\sqrt{r}$ and $k \to k$ for $k \in \mathbb{Z}$

ii. in $\mathbb{R}[x]$ the prime factorisation of $x^4 + x^2 r$ is $x^2(x^2 + r)$
Clearly $x, (x^2 + r)$ is irreducible in $\mathbb{R}[x]$ as $r > 0$
Hence from third isomorphism theorem we can say the residue of each factor of that polynomial will generated an ideal of $\frac{\mathbb{R}[x]}{\langle x^4+rx^2 \rangle}$ and vice-versa

Now there are 6 divisors hence total 6 ideals which are $\langle x \rangle, \langle x^2 \rangle, \langle x^2+r \rangle, \langle x(x^2+r) \rangle, \langle x^2(x^2+r) \rangle, \langle 1 \rangle$

Again we can say residue of each irreducible factors of $x^4 + rx^2$ in $\mathbb{C}[x]$ will generate a maximal ideal in $\frac{\mathbb{C}[x]}{\langle x^4+rx^2 \rangle}$ and vice versa
Now the prime factorisation of that polynomial in $\mathbb{C}[x]$ is $x^2(x - i\sqrt{r})(x + i\sqrt{r})$
Suince 3 irreducible factors hence 3 maximal ideals which are $\langle x \rangle, \langle x + i\sqrt{r} \rangle, \langle x - i\sqrt{r} \rangle$

iii. Now $\frac{1}{-r}x^2 + \frac{1}{r}(x^2 + r) = 1$ hence they are co prime

Hence

$$\frac{\mathbb{C}[x]}{\langle x^4+rx^2\rangle} \cong \frac{\mathbb{C}[x]}{\langle x^2\rangle} \times \frac{\mathbb{C}[x]}{\langle x^2+r\rangle}$$

again $\frac{1}{2i\sqrt{r}}[(x+i\sqrt{r})-(x-i\sqrt{r})]=1$ hence they are coprime
Hence

$$\frac{\mathbb{C}[x]}{\langle x^2+r\rangle} \cong \frac{\mathbb{C}[x]}{\langle x+i\sqrt{r}\rangle} \times \frac{\mathbb{C}[x]}{\langle x-i\sqrt{r}\rangle}$$

or,

$$\frac{\mathbb{C}[x]}{\langle x^4+rx^2\rangle} \cong \frac{\mathbb{C}[x]}{\langle x^2\rangle} \times \frac{\mathbb{C}[x]}{\langle x+i\sqrt{r}\rangle} \times \frac{\mathbb{C}[x]}{\langle x-i\sqrt{r}\rangle}$$

(We have applied CRT)

Question 4.

Degree of α over M is same as $[M(\alpha):M]$
Hence we have to find all possible value of $[M(\alpha):M]$
But $F \subseteq M$
Hence $F(\alpha) \subseteq M(\alpha)$
Again $M \subseteq F(\alpha)$
Hence $M(\alpha) \subseteq F(\alpha)$ as $\alpha \in \mathbb{F}(\alpha)$
Hence $M(\alpha) = F(\alpha)$
Or,

$$[M(\alpha):M] = [F(\alpha):M]$$

Now we know that

$$r^2 = [F(\alpha):F] = [F(\alpha):M] \times [M:F]$$

Hence $[F(\alpha):M]$ is a divisor of r^2

Now for any divisor d of r^2 we will find an example of M, F s.t. $[F(\alpha):M] = d$
And for this part we will take help from finite filed
Let for a prime p and $k \in \mathbb{N}$ $q = p^{r^2}$
Consider the field $\mathbb{F}_q$
Now we know that for any divisor d of r^2 we have $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_q$ and $[\mathbb{F}_q : \mathbb{F}_{p^d}]$
Hence $\mathbb{F}_{p^d} = M$

Hence possible values of $[M(\alpha):M]$ are all divisors of r^2

Question 5.

Let e be the 5^{th} root of unity and u be the real 5^{th} root of r
Now we know that the splitting field of $x^5 - r$ is irreducible in $\mathbb{Q}[x]$ as $r = 201954$ and $2 | r$ but $4 \not| r$
Now consider the extension $\mathbb{Q}(u)$, here we can write $p(x) = x^5 - r$ has a root u...........(i) and all other roots are complex
Now note the extension $\mathbb{Q}(u, e)$, we can see all the roots are here
(as in $\mathbb{C}[x]$ the roots are u, ue, ue^2, ue^3, ue^4)
Now we can say it is the smallest splitting field
Now $[\mathbb{Q}(u):\mathbb{Q}] = 5$ (from (i))
Now we know e is the root of $q(x) = x^4 + x^3 + x^2 + x + 1$

Now in question 6 We have proved that $q(x)$ is irreducible in $\mathbb{F}_2[x]$
Hence it is irreducible in $\mathbb{Q}[x]$
Hence $\left[\mathbb{Q}(e):\mathbb{Q}\right]=4$

Now we know that

$$4=\left[\mathbb{Q}(e):\mathbb{Q}\right]\Big|\left[\mathbb{Q}(u,e):\mathbb{Q}\right]$$

And

$$5=\left[\mathbb{Q}(u):\mathbb{Q}\right]\Big|\left[\mathbb{Q}(u,e):\mathbb{Q}\right]$$

Hence

$$20\Big|\left[\mathbb{Q}(u,e):\mathbb{Q}\right]$$

Also

$$\left[\mathbb{Q}(u,e):\mathbb{Q}\right]\leq\left[\mathbb{Q}(e):\mathbb{Q}\right]\times\left[\mathbb{Q}(u):\mathbb{Q}\right]=20$$

Hence

$$\left[\mathbb{Q}(u,e):\mathbb{Q}\right]=20$$

Question 6.

We will count the number of reducible 2 degree polynomials in $\mathbb{F}_p[x]$
Now if $p(x)\in\mathbb{F}_p[x]$ is reducible degree 2 then $p(x)=a(x-b)(x-c)$ for some $a,b,c\in\mathbb{F}_p, a\neq 0$
Now for $c\neq b$ we can choose a,b,c in $(p-1)^pC_2$ ways
For $c=b$ we can choose a,b,c in $p(p-1)$ ways
Now total number of degree 2 polynomials in $\mathbb{F}_p$ is $p^2(p-1)$
Hence total number of degree 2 irreducible polynomial $p^2(p-1)-p(p-1)-(p-1)^pC_2=(p^2-p-^pC_2)(p-1)==\frac{p(p-1)^2}{2}$
number of monic 2 degree irreducible polynomial in $\mathbb{F}_p[x]$ is $\frac{p(p-1)}{2}$

Now for degree 3
Let $p(x)$ is reducible degree 3 pol
One case can be $p(x)=(x-a)q(x)$, $q(x)$ is irreducible degree 2
Choice of such $p(x)$ is $p(p^2-p-^pC_2)(p-1)$
other case
$p(x)=d(x-a)(x-b)(x-c), a,b,c,d\in\mathbb{F}_p, d\neq 0$ for $a\neq b\neq c$ total cases $(p-1)^pC_3$
for $a\neq b, b=c$ total number of cases $p(p-1)^2$
for $a=b=c$ total number of cases $p(p-1)$

Total 3 degree polynomial $(p-1)p^3$
Hence total irreducible 3 degree polynomail is: $p^3(p-1)-(p(p-1)(p^2-p-^pC2)+p(p-1)^2+^pC3(p-1)+p(p-1))=\frac{p(p^2-1)(p-1)}{3}$
Hence number of monic 3 degree irreducible polynomial in $\mathbb{F}_p[x]$ is $\frac{p(p^2-1)}{3}$

Also one degree irreducible polynomials are p
Now $64=2^6$
divisors of 6 are $1,2,3,6$

Hence $x^{64}-x=$ product of all irreducible polynomial of degree 1,2,3,6 in $\mathbb{F}_2[x]$
Now the number of irreducible monic polynomial in $\mathbb{F}_2[x]$ of degree 2 is

$$\frac{64-1\times 2-2\times\frac{2(2-1)}{2}-3\times\frac{2(2^2-1)}{3}}{6}=9$$

Now $x^{64}-x=$ product of 2 irreducible degree 1 monic polynomial $\times$product of 1 irreducible degree 2 monic polynomial $\times$product of 2 irreducible degree 3 monic polynomial $\times$product of 9 irreducible degree 6 monic polynomial
And all of this irreducible factors are co prime since if we check in the splitting field of that polynomial then we will have 64 distinct root hence all such factors GCD will be 1
Now we know GCD does not change after field extension

Hence from CRT we can say $\mathbb{F}_2[x]/\langle x^{64}-x\rangle\cong(\mathbb{F}_2)^2\times(\mathbb{F}_4)\times(\mathbb{F}_8)^2\times(\mathbb{F}_{64})^9$
We know all fields of order 2^r is isomorphic to $\mathbb{F}_{2^r}$

Question 7.

We know 2017 is a prime
Our proof will be very much similar with the proof of existence of p^r order field
Now consider the polynomial $p(x)=x^r-x\in\mathbb{F}_{2017}[x]$
Since we knoe the existence of the splitting field we can say it will be $\mathbb{F}_{2017^n}$ for some $n\in\mathbb{N}$
We know that $p(x)$ has no multiple roots (as $p(x)$ and $p'(x)$ are co-prime) and the roots of $p(x)$ forms a subgroup in the splitting field (as if α,β are roots then so is $\alpha+\beta,\alpha\beta$)
Now that subgroup will be a cyclic group under multiplication as $\mathbb{F}^*_{2017^n}$ is a cyclic group under multiplication
Hence it has an element α whose order is r

Hence $r\big||\mathbb{F}^*_{2017^n}|=2017^n-1$
Hence we have to find minimum such n

Question 8.

Let $\mathbb{Q},E$ be as give and $\phi:E\to E$ be a homomorphism
Note since E is a field the kernel of the map will be either 0 or E but it cannot be E since 1 must map with 1
Hence the kernel is 0 hence the map is injective

Now since we have proved in the first problem that any homomorphism from $\mathbb{Q}$ (if exists) is unique
Hence $\phi\big|_{\mathbb{Q}}$ is a homomorphism and unique which is inclusion
Hence for any $\alpha\in E$ and $\alpha\in\mathbb{Q}$ has a preimage
Now for $\alpha\in E-\mathbb{Q}$ we have a irreducible polynomial $p(x)\in\mathbb{Q}[x]$ s.t. $p(\alpha)=0$
Now note $\phi(p(x))=p(\phi(x))$
Hence any root of $p(x)$ maps with a root of $p(x)$
Now if we restrict the map ϕ on the set of roots of $p(x)$ we can say it is also injective and the set of roots is non empty finite
Hence ϕ is surjective on that restriction

Hence α has a preimage
Hence ϕ is surjective

Now consider the map $\phi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ which sends $x \to x^2$ and $k \to k$ for $k \in \mathbb{Q}$
We can say it is not surjective since x has no preimage
Now from the universal property of fraction field we can extend it uniquely to $\tilde{\phi} : \mathbb{Q}(x) \to \mathbb{Q}(x)$ where $\tilde{\phi}\big|_{\mathbb{Q}[x]} = \phi$ and $\tilde{\phi}(p(x)^{-1}) = \phi^{-1}(x)$
Clearly x has no preimage w.r.t. $\tilde{\phi}$
Hence we have the counter example