MA3201 | Tut 1

(1.1) Given $v: K^* \to \mathbb{Z}$, $R = \{x \in K^* \mid v(x) \geq 0\}$, show $R$ is a subring of $K$ containing $1_K$.

Claim: $R$ is a subgp of $K$.

Let $x, y \in R$. We have $v(y) \geq 0$.

$\therefore v(y) + v(y) = v(y^2) \geq 0$.

$\therefore v(-y) + v(-y) \geq 0 \Rightarrow 2v(-y) \geq 0 \Rightarrow v(-y) \geq 0$.

$\therefore -y \in R$. WTS $x - y \in R$.

$v(x-y) \geq \min(v(x), v(-y)) \geq 0$. $\therefore x - y \in R$

$\therefore R$ is a subgp of $K$.

Claim: $R$ is closed under mult and is hence a subring of $K$.

$\forall x, y \in R$, $v(xy) = v(x) + v(y) \geq 0$.

Claim: $1 \in R$. $v(1 \cdot 1) = 2v(1) \Rightarrow v(1) = 0$.

$\forall x \in R$, $v(1 \cdot x) = v(1) + v(x) \geq 0$. Suppose $v(1) < 0$, we choose $y \in K^*$ s.t. $v(y) = -v(1)$ since $v$ is surjective. Then since $v(y) > 0$, $y \in R$. ~~...~~ But

$v(1 \cdot y) = v(y) + v(1) = 0 \rightarrow \epsilon$. $\square$

(1.2) Since $K$ is a field let $ab = 1$, $a, b \in K^*$.

$\therefore v(1) = v(a) + v(b)$. WTS $a \in R$ or $b \in R$.

~~...~~ We have $1 \in R$, so $v(a) + v(b) \geq 0 \Rightarrow$ ~~...~~ $a \notin R \wedge b \notin R$ is impossible

(1.3) ($\Leftarrow$) Suppose $v(x) = 0$. Then $v(1) = v(x) + v(x^{-1}) \geq 0$. $\Rightarrow v(x^{-1}) \geq 0$ $\Rightarrow x^{-1} \in R \Rightarrow x, x^{-1}$ are units in $R$.

($\Rightarrow$) $v(1) = v(x) + v(x^{-1}) = 0$. but both $x, x^{-1} \in R \Rightarrow v(x) = 0$.

MA3201 Tut 1 (2)

(2) We show $v_p : \mathbb{Q}^* \to \mathbb{Z}$, $\frac{a}{b} \mapsto \alpha$, $\frac{a}{b} = p^\alpha \frac{c}{d}$ $p \nmid c$, $p \nmid d$.

is a valuation ring.

<u>Claim: $v_p(ab) = v_p(a) + v_p(b)$ $\forall a, b \in \mathbb{Q}^*$</u>

Clearly $v_p(\frac{a}{b}\frac{c}{d}) = v_p(\frac{a'b'}{c'd'} p^{\alpha+\beta}) = \alpha+\beta$

where $v_p(\frac{a}{b}) = \frac{a'}{b'} p^\alpha$, $v_p(\frac{c}{d}) = \frac{c'}{d'} p^\beta$.

<u>Claim: $v_p$ is surjective</u>

Given any $n \in \mathbb{Z}$, we have $v_p(\frac{p^n}{1}) = n$.

<u>Claim: $v_p(a+b) \geq \min(v_p(a), v_p(b))$ for $a, b \in K^*$ s.t. $a+b \neq 0$.</u>

Let $v_p(\frac{a}{b}) = \alpha$, $v_p(\frac{c}{d}) = \beta$. WLOG let $\alpha < \beta$.

then $v_p(\frac{a}{b}+\frac{c}{d})$ ~~$= v_p(\frac{ad+bc}{bd})$~~

$= v_p(\frac{a'}{b'}p^\alpha + \frac{c'}{d'}p^\beta)$ ~~$= v_p(\frac{\quad}{b'd'})$~~

$= v_p(p^\alpha(\frac{a'}{b'} + \frac{c'}{d'}p^{\beta-\alpha}))$

$= \alpha + v_p(\frac{a'}{b'} + \frac{c'}{d'}p^{\beta-\alpha})$ note that denominator $p \nmid b'd'$.

$\geq \alpha = \min(v_p(\frac{a}{b}), v_p(\frac{c}{d}))$.

Q3 <u>Claim: $Z(R)$ is a subgroup</u>

Let $a, b \in Z(R)$. $\forall x \in R$, $x(a-b) = xa - xb$
$= ax - bx = (a-b)x$.

<u>Claim: $Z(R)$ is closed under $\times$</u>

Let $a, b \in Z(R)$. $\forall x \in R$, $x(ab) = xab = axb = (ab)x$.

<u>Claim: $Z(R)$ is comm.</u> follows from defn.

~~Q~~ MA3177 Tut (1) (3)

Q4. observe that $\phi_h$ ~~aa~~ $: G \to G$, $g \mapsto hg$ and $g \mapsto gh$ are bijections.
by cancellation laws of group $G$.

Then $\forall h \in G, r \in R$, $(rh) \cdot \sum_{g \in G} g = r \sum_{g \in G} hg = (\sum_{g \in G} gh) r$ (bijections)

$= (\sum_{g \in G} g)(rh)$

$\therefore \sum_{g \in G} g \in R[G]$. (or that conj. by an elem is an aut.)

Q5: we claim $Z(R[G]) = \{ \sum_{i=1}^{n} a_{C_i} (\sum_{g \in C_i} g) \mid C_1, \ldots, C_n$ are conj. classes in $G$, and $a_{C_i} \in R \}$.

every conj. class share a coefficient.

Let RHS $= Z'$. We check double inclusion.

WTS $Z(R[G]) \subseteq Z'$:

Let $x = \sum_{g \in G} a_g g \in Z(R[G])$. Since $x$ is in the center,
$\forall h \in G$, $hxh^{-1} = x$.

$= h(\sum a_g g) h^{-1} = \sum_{g \in G} h a_g g h^{-1}$.

$= \sum_{g \in G} a_g (hgh^{-1}) = \sum_{g \in G} a_g \cdot g$.

same.

$= \sum_{g \in G} a_{hgh^{-1}} (hgh^{-1})$

$\Rightarrow$ within conj. classes, the coeff are the same.

$\Rightarrow Z(R[G]) \subseteq Z'$.

WTS $Z' \subseteq Z(R[G])$.

This is clearly Q4.

MA3201 Tut 3

Q1. consider it in $\mathbb{Z}_2[x, y]$.

| $x$ | $y$ | $x^2+xy+1$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

$(x^2+1) + x(y)$.

consider it as $(\mathbb{Z}[x])[y]$,

we just need to show $(x^2+1)$ is prime in $\mathbb{Z}[x]$.

in fact, $\mathbb{Z}[x]$ ~~is~~ a UFD since $\mathbb{Z}$ is a UFD.

~~UFD~~ means prime $\Leftrightarrow$ irreducible. $x^2+1$ is irreducible in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Z}_3[x] \Rightarrow x^2+1$ is (irreducible) prime in $\mathbb{Z}[x]$

$\therefore$ By eisenstein's criterion, since $x = a_1 \notin (x^2+1)$, ~~a~~ $a_0 \in (x^2+1)$ but not $((x^2+1)^2)$, therefore $x^2+xy+1$ is irreducible.

~~Q2~~

Q2 (1) By eisenstein's criterion, with $p=2$, irreducible.

(2) ~~Substituting $x$ by any $f(x) \in R[x] \setminus R$, which is the map $a_nx^n + \dots + a_1x + a_0 \longmapsto a_nf(x)^n + \dots + a_1f(x) + a_0$ is an automorphism of $R[x]$.~~

Substituting $x$ by any non-zero-degree polynomial is an automorphism in $\mathbb{Z}[x]$, since the degree is not reduced $\Rightarrow$ kernel must have deg 1 and any $x$ in is not substituted $\Rightarrow$ $\ker = \{0\}$.

$\therefore$ $(x+1)^4+1$ is irreducible $\Rightarrow$ $x^4+1$ is irreducible.

Q3. (1) WTS $M_c$ is a max ideal of $R$.

Ideal: $0-0=0$, $0 \cdot 0 = 0$, $k \cdot 0 = 0$. $f(x) = 0 \in M_c$ is not empty.

Maximal: Let any $J$ properly contain $M_c$. We claim $1 \in J$.

Suppose $g \in J \setminus M_c \Rightarrow g(c) \neq 0 \Rightarrow h(x) := g(x)/g(c) \in J$.

$1 - h(c) = 0 \Rightarrow (1-h(x)) \in M_c \subsetneq J \Rightarrow [1-h(x)] + h(x) \in J$ (ring).

$\Rightarrow 1 \in J$ $\square$

Q 3.(2) Suppose the contrary, let $M$ such that $M \neq M_c$ and $M$ maximal.
Then $\forall c \in [0,1]$, $\exists f \in M$ s.t. $f(c) \neq 0$. By continuity, $\exists$ interval around $c$ such that $f(V_c) \neq 0$. Now the open covering of $[0,1]$, $G = \{V_c \subset [0,1]\}$ must have a finite subcover by completeness of $\mathbb{R}$. I.e:

$$[0,1] \supseteq V_1 \cup V_2 \cup \dots \cup V_n \text{ for some intervals } V_i.$$

Denote the function $f_i$ s.t. $f(x_i) \neq 0$. $\forall x \in V_i$.

~~let $g(x) := f_1(x_1)^2 + \dots + f(x_n)^2$~~

let $g := f_1^2 + f_2^2 + \dots + f_n^2$. Then $g(x) > 0$ $\forall x \in [0,1]$

$\therefore g \in M$. $1/g \in M$. $\Rightarrow 1 \in M$ ($\rightarrow\leftarrow$). $\square$.

~~Q4.~~

Q4. Ring: Abelian gp: $a^{op} + (a')^{op} = 0^{op} \Rightarrow (a+a')^{op} = 0^{op}$ (identity.)

by bijection, $a + a' = 0 \Rightarrow a' = -a$. (inv).

(assoc): $a^{op} + b^{op} + c^{op} = (a+b)^{op} + c^{op} = (a+b+c)^{op} = a^{op} + (b^{op} + c^{op})$

Mult: closed is natural. assoc is by underlying op:

$$a^{op} b^{op} c^{op} = (ba)^{op} c^{op} = (cba)^{op} = a^{op} (bc)^{op}.$$

dist: $a^{op}(b^{op} + c^{op}) = [(b+c)a]^{op} = a^{op} b^{op} + a^{op} c^{op}$

$(a^{op} + b^{op}) c^{op} = [c(a+b)]^{op} = a^{op} c^{op} + b^{op} c^{op}$.

Mult. id: then $a^{op} 1^{op} = (1 \cdot a)^{op} = (a \cdot 1)^{op} = 1^{op} a^{op} = a^{op}$.

Module: Let $M$ be a $R$-module (left). Then the action $(r, m) \longmapsto r \cdot m$ can canonically induce $(m, r^{op}) \longmapsto r \cdot m$, $M \times R^{op} \longmapsto M$.

1. $(m+n) \cdot r^{op} = r \cdot (m+n) = r \cdot m + r \cdot n = m \cdot r^{op} + n \cdot r^{op}$.
2. $m \cdot (r^{op} + s^{op}) = m \cdot (r+s)^{op} = (r+s) \cdot m = r \cdot m + s \cdot m = m \cdot r^{op} + m \cdot s^{op}$
3. $m \cdot (s^{op} \cdot r^{op}) = m \cdot (sr)^{op} = (sr)(m) = s \cdot (r \cdot m) = s \cdot (m \cdot r^{op})$
$= (m \cdot r^{op})^{op} \cdot s^{op}$ $\square$
4. $m \cdot (1^{op}) = 1 \cdot m = m$.

MA3201 Tut 3 (2)

Q5. Let $I$ be an index set, $N = \bigcap_{c \in I} M_c$ where $M_c$ are submods of a $R$-mod $M$. Clearly $N$ is an abelian subgp of $M$, and we verify that $N$ is closed under action of $R$: $\forall r \in R$, $n \in N$. $n \in M_c \; \forall c \in I$.

$r \cdot n \in M_c \; \forall c \in I$ since $M_c$ is a submod of $N$.

$\Rightarrow r \cdot n \in \bigcap_{c \in I} M_c = N$ $\square$.

Q6. Let $N = \bigcup_{i=1}^{\infty} N_i$. We verify $N$ is an Ab. gp closed under action of $R$.

Ab. gp: $\forall x, y \in N$, $x \in N_a$, $y \in N_b$ for some $a, b \in \mathbb{N}$.

Then $x, y \in N_{\max(a,b)}$ which is an Ab gp.

Closed: $\forall x \in N$, $x \in N_a$, $\forall r \in R$, $r \cdot x \in N_a \subset N$. $\square$.