Solutions to MA5020 – Abstract Algebra 240308

Exercise 1

(a) False: Let $G = D_8$ $H = \langle (1,2,3,4) \rangle$ $N = \langle (13)(24) \rangle$

Then $[G:H] = 2$ so $H \trianglelefteq G$ H is abelian so $N \trianglelefteq H$

$(12)[(13)(24)](12) = (14)(23) \notin N \Rightarrow N \not\trianglelefteq G$

(b) This is again false

S_3 is not abelian $S_3/\langle (1,23) \rangle \cong \mathbb{Z}_2$

Exercise 2

(a) since either one is normal we have that $NM < G$

Let now $g \in G$ $nm \in NM$ with $n \in N$ $m \in M$

$gn \cdot mg^{-1} = n'gmg^{-1}$ for some $n' \in N$ since $N \trianglelefteq G$ and so $gng^{-1} = n' \in N$

$= n' \cdot m'$ for some $m' \in M$ since $M \trianglelefteq G$

$\in NM \trianglelefteq G$

(b) We show first that for $n \in N$ and $m \in N$ $n \cdot m = mn$

Consider $n \cdot m n^{-1} m^{-1} = (nmn^{-1}) m^{-1} = m' \cdot m^{-1}$ for some $m' \in M$ since $M \trianglelefteq G$

$\in M$

$n(mn^{-1}m^{-1}) = nn' \in N$ for some $n' \in N$ since $N \trianglelefteq G$

$\Rightarrow n \cdot mn^{-1} \cdot m^{-1} \in M \cap N = \{e\} \Rightarrow nm = mn$

Now we define

$\varphi : \begin{array}{ccc} N \times M & \longrightarrow & G \\ (n,m) & \longmapsto & n \cdot m \end{array}$ This is a group homomorphism

$\varphi((n,m)(a,b)) = \varphi((na, mb)) = na \cdot mb \overset{*}{=} nm \cdot ab = \varphi(nm) \cdot \varphi(a,b)$

* elements in N and M commute

φ is onto since $NM = G$

φ is injective since

$\ker \varphi = \{(n,m) \mid nm = 1\} = \{(n, n^{-1}) \mid n \in N \; n^{-1} \in M\} = \{(n, n^{-1}) \mid n \in M \cap N\} = \{(1,1)\}$

(c) there is a unique $P \in Syl_3(G)$ and a unique $Q \in Syl_5(G)$. Since G is abelian we have that $P, Q \trianglelefteq G$ and $P \cap Q = \{1\}$

$|P \cdot Q| = |P| \cdot |Q| = 3 \cdot 25 = 75 = |G| \Rightarrow PQ = G$

$G \cong P \times Q$ $\quad P \cong \mathbb{Z}/3\mathbb{Z}$

$Q \cong (\mathbb{Z}/5\mathbb{Z})^2$ or $(\mathbb{Z}/25\mathbb{Z})$

$G \cong \mathbb{Z}/75$ or $\mathbb{Z}/15 \cdot \mathbb{Z}/5 \cong \mathbb{Z}/3 \times (\mathbb{Z}/5)^2$

Exercise 3

(a) $\Theta_x = \{x\} \subset \Omega \Rightarrow gx = x$ for all $x \in G \Leftrightarrow x \in X^G$

(b) $X = \bigcup_{\Theta} \Theta$ Θ orbit

$= \bigcup_{x \in X^G} \{x\} \cup \bigcup_{x \notin X^G} \Theta_x$

$\Rightarrow |X| = |X^G| + \sum |\Theta_i|$ by the orbit stabilizer thm

$= |X^G| + \sum [G : G_{y_i}]$ for $y_i \in \Theta_i$

Since G is a p-group $[G : G_y] = 1$ or p^m $m > 0$

but we can exclude the first, since otherwise we would have $y \in X^G$ by (a)

$\Rightarrow X \equiv |X^G| \mod p$

Exercise 4

(a) $P \trianglelefteq G$ thus $gPg^{-1} = P$ and for all $g \in P$ we have

$G \longrightarrow Aut(P) \cong \mathbb{Z}/4\mathbb{Z}$

$g \longmapsto \sigma_g : P \longrightarrow P$
$\quad\quad\quad\quad\quad\quad\quad\quad p \longmapsto gpg^{-1}$

If this is not trivial then a quotient of G is a nontrivial subgroup of $\mathbb{Z}/4\mathbb{Z}$

$\Rightarrow$ a quotient of G has even order. But this is impossible as $2 \nmid |G|$

(b) $n_{13} \equiv 1 \mod 13$ $\quad n_{13} \mid 27$ $\quad \Rightarrow n_{13} = 1, 27$

Suppose by contradiction that G is simple, so that $n_{13} = 27$. Then we have $27 \cdot 12$ elements of order 13. This leaves space only for other 27 elements whose order divides 3 $\quad Q_1, Q_2 \subset Syl_3(G) \Rightarrow Q_1 = G \setminus \{\text{elements of order } 13\}$

$= Q_2$

Exercise 5

(a) We need to check that

(1) $x+y \in \mathfrak{N}$ for all $x, y \in \mathfrak{N}$
(2) $0 \in \mathfrak{N}$
(3) $\lambda x \in \mathfrak{N}$ for all $\lambda \in R$ and all $x \in \mathfrak{N}$

(2) is trivial $0^n = 0$ for all $n > 0$

(3) $\lambda \in R$ $x \in \mathfrak{N}$ let $n > 0$ such that $x^n = 0$. Then $(\lambda x)^n = \lambda^n \cdot x^n = \lambda^n \cdot 0 = 0$

(1) Let $x, y \in \mathfrak{N}$ and let $m, k \in \mathbb{Z}_{>0}$ such that $x^m = 0$ $y^k = 0$

$$(x+y)^{m+k} = \sum_{i=0}^{m+k} \binom{m+k}{i} x^i y^{m+k-i} = \sum_{i=0}^{m} \binom{m+k}{i} x^i y^{k+(m-i)} + \sum_{i=m+1}^{m+k} \binom{m+k}{i} x^{i-m} \cdot y^{m+k-i}$$

$$= \sum_{i=0}^{m} \binom{m+k}{i} x^i \cdot 0 + \sum_{i=m+1}^{m+k} \binom{m+k}{i} 0 \cdot y^{m+k-i} = 0$$

(b) Suppose that $x^n = 0$ for some $n > 0$ and let $\mathfrak{p}$ a prime ideal

we are going to show that $x \in \mathfrak{p}$.

We will show by induction on $n \geq 0$ that $x^n \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$

For $n = 1$ we have $x^1 \in \mathfrak{p} \iff x \in \mathfrak{p}$ and the statement is correct

Suppose that the statement is true for $n = k$ and let us prove it for $n = k+1$

Let $x^{k+1} \in \mathfrak{p}$ $x^{k+1} = (x^k) \cdot x \in \mathfrak{p}$ if $x \notin \mathfrak{p}$ then $x^k \in \mathfrak{p}$ and by induction $x \in \mathfrak{p}$

Thus $x^n = 0 \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$.

Exercise 6

(a) $\alpha = 2\sqrt{3} - \sqrt{5} \Rightarrow \alpha^2 = 12 + 5 - 4\sqrt{15} \Rightarrow (\alpha^2 - 17) = -4\sqrt{15}$

$$\alpha^4 - 34\alpha^2 + 17^2 = 16 \cdot 5 \Rightarrow \alpha^4 - 34\alpha^2 + 49 = 0$$

Thus we have that $x^4 - 34x^2 + 49$ has a root in α. It is monic, thus we only have to show irreducibility.

We see that the possible rational roots are ± 1 ± 7 ± 49 and none of those work

Thus $p(x)$ can only be factored as

$$(x^2 + ax + b)(x^2 + a'x + b')$$

which gives us

$$\begin{cases} a + a' = 0 \\ aa' + b + b' = -34 \\ ab' + a'b = 0 \\ b'b = 49 \end{cases}$$

If $a = a' = 0$ then by setting $y = x^2$ we would have that

$y^2 - 34y + 49 = (y+b)(y+b')$ has rational roots but this is not the case

Thus $a \neq 0 \Rightarrow b = b'$ and $b^2 = 49$

The only possibilities are $b = \pm 7$

$b = 7$ yields $-a^2 + 14 = -34$ $a^2 = +58$ which has no solution for $a \in \mathbb{Q}$ $b = -7$ yields $-a^2 - 14 = -34$ $a^2 = 20$ which again has no solution for $a \in \mathbb{Q}$

(b) $[\mathbb{Q}(2\sqrt{3} - \sqrt{5}) : \mathbb{Q}]$ = degree of the minimal polynomial of $2\sqrt{3} - \sqrt{5}$

$= 4$

A Basis is given by

$1, \ 2\sqrt{3} - \sqrt{5}, \ 17 - 4\sqrt{15} = (2\sqrt{3} - \sqrt{5})^2, \ (2\sqrt{3} - \sqrt{5})^3 = (17 - 4\sqrt{15})(2\sqrt{3} - \sqrt{5})$

$= 34\sqrt{3} - 17\sqrt{5} - 24\sqrt{5} + 20\sqrt{3}$

$= 54\sqrt{3} - 41\sqrt{5}$

(c) Method 1

$2\sqrt{3} - \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5}) \Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{5}) \geq \mathbb{Q}(2\sqrt{3} - \sqrt{5})$

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(2\sqrt{3} - \sqrt{5})]}_{\lambda \geq 1} \cdot \underbrace{[\mathbb{Q}(2\sqrt{3} - \sqrt{5}) : \mathbb{Q}]}_{4}$

We want to show that $\lambda = 1$

$\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3})(\sqrt{5})$

The minimal polynomial of $\sqrt{3}$ / $\mathbb{Q}$ is $x^2 - 3$ $\Rightarrow [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$

We have that $\sqrt{5}$ is a root of $x^2 - 5$ / $\mathbb{Q}(\sqrt{3})$ so $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] \leq 2$

We deduce that

$[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \leq 4$

So $4 \geq \lambda \cdot 4 \Rightarrow \lambda = 1$

Method 2 $2\sqrt{3} - \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5}) \Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{5}) \geq \mathbb{Q}(2\sqrt{3} - \sqrt{5})$

$\sqrt{3} = \frac{41}{24}(2\sqrt{3} - \sqrt{5}) - \frac{1}{24}(2\sqrt{3} - \sqrt{5})^3 \in \mathbb{Q}(2\sqrt{3} - \sqrt{5})$

$\sqrt{5} = \frac{27}{14}(2\sqrt{3} - \sqrt{5}) - \frac{1}{14}(2\sqrt{3} - \sqrt{5})^3 \in \mathbb{Q}(2\sqrt{3} - \sqrt{5})$

$\Rightarrow \mathbb{Q}(\sqrt{3}, \sqrt{5}) \leq \mathbb{Q}(2\sqrt{3} - \sqrt{5})$