Solutions to exam in algebra MMG500

2017-03-17

1a) $\mathbf{Z}_6 \times \mathbf{Z}_2$ is abelian of order 12, but not cyclic as $6a=0$ for every $a \in \mathbf{Z}_6 \times \mathbf{Z}_2$.
b) $S_3 \times \mathbf{Z}_2$ is non-abelian of order 12 as S_3 is non-abelian of order 6.

2a) $\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(\mathrm{id}) = e$ as φ is a homomorphism. As $o(H)=3$, we have also that $\varphi(\tau)^3 = e$ by a theorem. So $\varphi(\tau) = e$ such that τ of order one.

b) As any element in S_n is a product of transpositions we deduce from a) that Im $\varphi = \{e\}$ for any homomorphism $\varphi: S_n \rightarrow H$ to a group of order 3. But the quotient map $\varphi: S_n \rightarrow S_n/N$ of a normal subgroup is always surjective. There can thus be no normal subgroup of index 3 in S_n as otherwise we would have a contradiction.

3. We first note that $(2a)^2 + 3(2b)^2 \equiv 0 \pmod 4$ as $(2a)^2 \equiv (2b)^2 \equiv 0 \pmod 4$ when $2a$ and $2b$ are even and as $(2a)^2 \equiv (2b)^2 \equiv 1 \pmod 4$ when $2a$ and $2b$ are odd. Hence $N(z) := |z|^2 = a^2 + 3b^2 \in \mathbf{N}$ for any $z = a + b\sqrt{3}i \in R$ different from 0. So if z is a unit in R with inverse w, then $N(z) = 1$ as $N(z)N(w) = N(zw) = N(1) = 1$. Hence $(2a)^2 + 3(2b)^2 = N(2z) = N(2)N(z) = 4$, which implies that $(2a)^2 = 4$ and $(2b)^2 = 0$ or that $(2a)^2 = (2b)^2 = 1$. There are thus at most six possible units given by ± 1 and $\pm 1/2 \pm \sqrt{3}i/2$. These are all units in R as they correspond to the six roots of the equation $z^6 = 1$.

4a) α belongs to the multiplicative group $U(K) = K \setminus \{0\}$ of order 3. Hence $\alpha^3 = 1$ and $\alpha^{2017} = \alpha^{2016}\alpha = (\alpha^3)^{672}\alpha = \alpha$.

b) $\alpha^{2018} + \alpha^{2017} + 1 = \alpha^{2017}\alpha + \alpha + 1 = \alpha^2 + \alpha + 1 = (\alpha^3 - 1)/(\alpha - 1) = 0$ as $\alpha \notin \{0.1\}$.

c) It follows from the factor theorem that $x^{2018} + x^{2017} + 1$ is divisible by $x - \alpha$ as it has a zero at $\alpha \in K$. The polynomial is thus not irreducible over K

5. See Durbin's book.

6. See Durbin's book.