Solutions to exam in algebra (MMG 500 & MVE 150) 2018-08-22

1a) The 2×2-matrices $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ in GL(2, $\mathbf{Z}_2$) are those where either $a_{11}\,a_{22}=1$ and $a_{12}\,a_{21}=0$ or where $a_{11}\,a_{22}=0$ and $a_{12}\,a_{21}=1$. In the first case we get that $a_{11}=a_{22}=1$ and that a_{12} or $a_{21}=0$. In the second case we get that a_{11} or $a_{22}=0$ and that $a_{11}=a_{22}=1$. There are thus 3+3 matrices in GL(2, $\mathbf{Z}_2$) , such that GL(2, $\mathbf{Z}_2$) is a group of order 6.

b) We have two trivial normal subgroups, namely GL(2, $\mathbf{Z}_2$) itself and the group with the neutral element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The other subgroups are of order 2 or 3 by Lagrange's theorem. By a corollary of the same theorem they are therefore cyclic as they are of prime order. They are thus generated by an element of order 2 o 3. There are exactly three elements of order two given by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. None of these are in the center of GL(2, $\mathbf{Z}_2$) as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Their conjugacy classes must therefore consist of more than one element, which means that none of these three elements can generate a normal subgroup. There are thus no normal subgroups of order 2. The only subgroup or order 3 is the subgroup H consisting of $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and the elements $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ of order 3. This is normal as their conjugates must have the same order. There is thus only normal subgroup in GL(2, $\mathbf{Z}_2$) apart from the trivial ones.

2a) It follows from the associative law for matrix multiplication that

$$\left(\left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\right)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\left(\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right)\right)$$

for all $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ in GL(2,F) and all $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ in S.

If we write π_A: $S \to S$ for the map which sends $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ to $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, then we thus have that $\pi_{AB} = \pi_A \circ \pi_B$ such that π is a group action of GL(2, $\boldsymbol{F}$) on S.

(b) As $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ the column vectors

$\begin{pmatrix}0\\1\end{pmatrix}$, $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}1\\1\end{pmatrix}$ are in the orbit of $\begin{pmatrix}1\\0\end{pmatrix}$ .These are all elements of the orbit as $\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$ would imply that $\begin{pmatrix}a_{11}\\ a_{21}\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$ and $\begin{vmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}=0$.

2b) As $\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}a_{11}\\ a_{21}\end{pmatrix}$ we see that the stabiliser of $\begin{pmatrix}1\\0\end{pmatrix}$ consists of the matrices in GL(2, $\mathbf{Z}_2$) of the form $\begin{pmatrix}1 & a_{12}\\ 0 & a_{22}\end{pmatrix}$. But then we get from $\begin{vmatrix}1 & a_{12}\\ 0 & a_{22}\end{vmatrix}\neq 0$ that $a_{22}=1$.The stabilizer of $\begin{pmatrix}1\\0\end{pmatrix}$ will therefore consisr of the two binary matrices $\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$ where a= 0 or 1.

3) We first verify that $\varphi^{-1}(J)$ is an additive subgroup of R_1. Clearly $\varphi^{-1}(J)\neq\varnothing$ as $\varphi(0)=0\in J$. We have also if $a,b\in\varphi^{-1}(J)$, that $\varphi(a+b)=\varphi(a)+\varphi(b)\in J$ and $\varphi(-a)=-\varphi(a)\in J$ as J is an additive subgroup of R_2. Hence $a,b\in\varphi^{-1}(J)$ implies that $a+b$, $-a\in\varphi^{-1}(J)$ such that $\varphi^{-1}(J)$ is an additive subgroup of R_1 by the subgroup criterion.

To see that $\varphi^{-1}(J)$ is an ideal of R_1 , suppose that $r\in R_1$ and $i\in\varphi^{-1}(J)$. Then $\varphi(r\,i)=\varphi(r)\,\varphi(i)$ with $\varphi(i)\in J$. But then as $\varphi(i)$ belong to the ideal J in R_2 , we get that $\varphi(r\,i)=\varphi(r)\,\varphi(i)\in J$ and $ri\in\varphi^{-1}(J)$. This shows that $\varphi^{-1}(J)$ is an ideal of R_1.

4a) As $(a+b\sqrt{p})+(c+d\sqrt{p})=(a+c)+(b+d)\sqrt{p}$, $(a+b\sqrt{p})-(c+d\sqrt{p})=(a-c)+(b-d)\sqrt{p}$, and $(a+b\sqrt{p})(c+d\sqrt{p})=(ac+pbd)+(ad+bc)\sqrt{p}$, we see that $\mathbf{Q}(\sqrt{p})$ is closed under addition subtraction and multiplication.It is therefore a subring of $\mathbf{Q}(\sqrt{p})$ by the subring criterion. We have also the multiplicative inverse $(a-b\sqrt{p})/(a^2-pb^2)$ to any element $a+b\sqrt{p}\neq 0$ in $\mathbf{Q}(\sqrt{p})$. Hence $\mathbf{Q}(\sqrt{p})$ is a subfield of **R.**

4b) Suppose we had a ring isomorphism ϕ from $\mathbf{Q}(\sqrt{q})$ **to** $\mathbf{Q}(\sqrt{p})$ for two different primes primes p.and q. We may then find rational number a and b with $\phi(\sqrt{q})=a+b\sqrt{p}$. But then $q=\phi(q)=(\phi(\sqrt{q})^2=(a+b\sqrt{p})^2=(a^2+b^2p)+2ab\sqrt{p}$. If now $ab\neq 0$, then we would have that $\sqrt{p}\in\mathbf{Q}$. Otherwise, either a=0 and $\sqrt{pq}=\pm bp\in\mathbf{Q}$ or b=0 and $\sqrt{q}=\pm a\in\mathbf{Q}$. We have thus shown that one of $\sqrt{p}$, $\sqrt{pq}$ or $\sqrt{q}$ must be rational if $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{q})$ are isomorphic as fields. But if r >I is an square-free integer, then $\sqrt{r}$ cannot be rational as $\sqrt{r}=m/n$ would lead to $rn^2=m^2$ and that all exponents in the prime factorizations of rn^2 are even. But this is a contradiction. Hence $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\sqrt{q})$ cannot be isomorphic as fields.

5] See Durbin's book

6) See Durbin´´s book