MATHEMATICS
Univ. of Gothenburg and Chalmers University of Technology
Examination in algebra: MMG 500 and MVE 150, 2020-06-08.
Telephone 031-41 46 70

1) Let G be the set of all 2×2-matrices of the form $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ where

$a\neq 0$ and b are real numbers . Show that G is a group with respect to matrix multiplication. 3p

2) Let $\mathbf{H}=\{z\in\mathbf{C}\colon \mathrm{Im}(z)>0\}$ be the set of complex numbers in the upper half plane and G be the group in 1). For $g=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\in G$, let $\pi_g\colon \mathbf{H}\to\mathbf{C}$ be the map which sends z to $a^2 z+ab$.

(a) Prove that π_g is a permutation of $\mathbf{H}$ for all $g\in G$ and that these permutations define an action of G on $\mathbf{H}$. 3p

(b) Determine the stabiliser of i in G. 1p

(d) Prove that G acts transitively on $\mathbf{H}$. 2p

3) Let G be a group with only one element h of order 2. 3p
Prove that $gh=hg$ for all $g\in G$.

4) Let I be the principal ideal in $\mathbf{Z}_2[x]$ generated by x^3+x+1. 4p
Compute $(f(x)+I)^2\in\mathbf{Z}_2[x]/I$ for all binary polynomials $f(x)$ of degree two. (The .answers should be given in the form $g(x)+I$ with $g(x)$ of degree at most two.)

5) Let $K=\mathbf{Q}[x]/I$ for the principal ideal $I=(x^3-2)$.

a) Show that K is a field. 2p

b) Determine all field homomorphisms from K to $\mathbf{C}$. 3p

6) The largest known prime to date is $p=2^{82\,589\,933}-1$. Find all the roots in $\mathbf{Z}_p$ to the equation $x^{82\,589\,932}+x^{82\,589\,931}+\ldots+x^2+x+1=0$. 4p

You may use the theorems in Durbin's book to solve the exercises.
But all claims should be motivated!

Solutions to examination in algebra: MMG500 /MVE 150, 2020-06-08.

1) G is closed under multiplication as $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}=\begin{pmatrix} ac & ad+bc^{-1} \\ 0 & (ac)^{-1} \end{pmatrix} \in G$

The operation is associative as matrix multiplication is associative and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is a neutral element as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$.

Finally. as $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}=\begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ we see that all elements in G have inverses in G such that all four group axioms hold.

2a) $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}z\in\mathbf{H}$ for $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\in G$ and $z\in\mathbf{H}$ as $\mathrm{Im}(a^2\mathrm{z}+ab)= a^2\ \mathrm{Im(z)}>0$. The map which sends z to $w=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}z$ is a permutation on $\mathbf{H}$ as there is an inverse map given by $z=\begin{pmatrix} a^{-1} & -b \\ 0 & a \end{pmatrix}w= a^{-2}\mathrm{w}-ab$.

Further, $\left(\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}\right)z=\begin{pmatrix} ac & ad+bc^{-1} \\ 0 & (ac)^{-1} \end{pmatrix}z=(ac)^2\mathrm{z}+ ac(ad+b/c)$ while $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}\left(\begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix}z\right)=\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}(c^2\mathrm{z}+cd)= a^2(c^2\mathrm{z}+cd)+ab=(ac)^2\mathrm{z}+ ac(ad+b/c)$.

Hence the map which sends z to $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}z$ is an action of G on $\mathbf{H}$.

$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ is in the stabiliser of i if and only if $a^2i+ab= i$. By separating the real and imaginary parts we have thus that $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ is in the stabiliser of i if and only if $a^2=1$ and $ab=0$ which means that $a=\pm1$ and $b=0$. There are thus just two matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ in the stabilizer of i.

(c) The orbit of i consists of all complex number of the form $b+a^2i$ where $a\neq0$ and b are arbitrary real numbers. The orbit of i is thus $\mathbf{H}$ and the action transitive.

3) $(ghg^{-1})^2 = ghg^{-1}ghg^{-1} = ghh\,g^{-1} = ge\,g^{-1} = e$. This means that ghg^{-1} is of order two as $ghg^{-1}=e$ would imply that $h = g^{-1}e\,g = e$. As h is the only one element of order 2 we have this that $ghg^{-1}=h$ and $gh=hg$ for all $g\in G$.

4) If a,b,c, are elements in a ring R of characteristic two, then $(a+b+c)^2 = a^2+b^2+c^2+2(ab+ac+bc) = a^2+b^2+c^2$. As char($\mathbf{Z}_2[x]$)=2, we have therefore that $(x^2+Ax+B)^2 = x^4+A^2x^2+B^2 = x^4+Ax^2+B$ in $\mathbf{Z}_2[x]$ for any $A,B \in \mathbf{Z}_2$.
Further, $x^4+I = x^2+x+I$ as $x^4 - x^2 - x = x^4+x^2+x = x(x^3+x+1)\in I$. Therefore,
$(x^2+Ax+B+I)^2 = (x^2+Ax+B)^2+I = x^4+Ax^2+B+I = (A+1)\,x^2+x+B+I$ for $A, B \in \mathbf{Z}_2$.
Hence, $(x^2+I)^2 = x^2+x+I$, $(x^2+1+I)^2 = x^2+x+1+I$, $(x^2+x+I)^2 = x+I$ and $(x^2+x+1+I)^2 = x+1+I$.

5a) Suppose that $f(x) = x^3-2$ had a root α in $\mathbf{Q}$. Then $\alpha = m/n$ for two coprime integers with $m^3=2n^3$. But then m must be even $2n^3 = m^3$ be divisible by 4 and n also be even. As this is a contradiction , $f(x)$ has thus no root in $\mathbf{Q}$ and no linear factor in $\mathbf{Q}[x]$, It is therefore irreducible over $\mathbf{Q}$ as deg f=3. (This can also be seen from the Eisenstein criterion,.)
As $f(x)$ is irreducible over $\mathbf{Q}$, we have thus by theorem 42.3 in Durbin's book that $K = \mathbf{Q}[x]/(f(x))$ is a field.
b) If ϕ: $\mathbf{Q}[x]/I \to \mathbf{C}$ is a ring homomorphism, then

$$\phi(x+I)^3 = \phi(x^3+I) = \phi(x^3+I) = \phi(2+I) = \phi(1+I)+\phi(1+I) = 1+1=2$$

such that $\phi(x+I)\in\{\sqrt[3]{2}, \sqrt[3]{2}(-1+\iota\sqrt{3}), \sqrt[3]{2}(-1-\iota\sqrt{3})/2\}$.
But any coset in $\mathbf{Q}[x]/I$ can be represented by a quadratic polynomial Ax^2+Bx+C in $\mathbf{Q}[x]$ and $\phi(Ax^2+Bx+C+I) = A\phi(x+I)^2+B\phi(x+I)+C$ The homomorphism θ is therefore uniquely determined by $\phi(x+I)$.
If conversely $\beta \in \mathbf{C}$, then we have a ring homomorphism θ from $\mathbf{Q}[x]$ to $\mathbf{C}$, which sends $g(x)\in\mathbf{Q}[x]$ to $g(\beta)$. If $\beta\in\{\sqrt[3]{2}, \sqrt[3]{2}(-1+\iota\sqrt{3}), \sqrt[3]{2}(-1-\iota\sqrt{3})/2\}$, then we have further that $\theta(x^3-2) = \beta^3-2=0$ such that $I=(x^3-2)\subseteq\ker\theta$. There exists therefore by the fundamental homomorphism theorem for rings (see Durbin p.178) a ring homomorphsim ϕ from $\mathbf{Q}[x]/I$ to $\mathbf{C}$, which sends $g(x)+I$ to $\theta(g(x)) = g(\beta)$ and $x+I$ to β. There are therefore exactly three ring homomophisms from $K = \mathbf{Q}[x]/I$ to C.

6) Let q=82 589 933 and $[a]$ be the congruence class of a(mod p) for $a \in \mathbf{Z}$.
Then $[2^k]^q = [2^{kq}] = [2^q]^k = [1]^k = [1]$ for any integer k. The polynomial $x^q - 1$
has thus q different zeroes in $\mathbf{Z}_p$ given by $[1], [2], [2^2], \ldots, [2^{q-1}]$.
Now let $f(x) = x^{q-1} + {}^{q-2} + \ldots + x^2 + x + 1$. Then $f(x)(x-1) = x^q - 1$ in $\mathbf{Z}$ and hence
also in $\mathbf{Z}_p$. This means that any zero of $f(x)$ in $\mathbf{Z}_p$ will be a zero of $x^q - 1$. If conversely $[a] \neq [1]$ is a zero of $x^q - 1$, then $f([a])([a]-[1]) = [0]$ and $[a]-[1] \neq [0]$
in $\mathbf{Z}_p$. But then $f([a]) = [0]$ as $\mathbf{Z}_p$ an integral domain (an even a field) for a prime p. We have therefore shown that $[2], [2^2], \ldots, [2^{q-1}]$ are zeroes of $f(x)$ in $\mathbf{Z}_p$.
These are then all zeroes by theorem 43.1.