MATH3303: 2015 FINAL EXAM

(1) Show that $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic if and only if $\gcd(m, n) = 1$.

Solution. The group in question consists of mn elements:

$$G := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} = \{(a, b) : a \in \mathbb{Z}/m\mathbb{Z},\ b \in \mathbb{Z}/n\mathbb{Z}\}$$

and is equipped with the multiplication $(a, b) \cdot (c, d) = (ac, bd)$. Clearly, G has order mn. The element $(a, b) \in G$ will be a generator of G iff a generates $\mathbb{Z}/m\mathbb{Z}$, b generates $\mathbb{Z}/n\mathbb{Z}$ and $(a, b)^i = (a^i, b^i) \neq (1, 1) = 1_G$ for $1 \leq i < mn$. Since m, n are the smallest positive integers for which $a^m = 1$ and $b^n = 1$, the smallest positive i for which $(a^i, b^i) = (1, 1)$ will be $i = \operatorname{lcm}(m, n)$. Hence (a, b) generates G iff $\operatorname{lcm}(m, n) = mn$. Since (for positive m, n) $\operatorname{lcm}(m, n) \gcd(m, n) = mn$ we must thus have $\gcd(m, n) = 1$.

(2) Let G be a group and H be a subgroup of G. Suppose the order of $|G/H| = 2$. Show that H is normal in G.

Solution. Note: As stated the question is not 100% kosher, since G/H is only a group (and hence has a well-defined order) if H is a normal subgroup. It should have said "Suppose $[G : H] = 2$."
We know that H partitions G into right (left) cosets. If the index of H in G is two, there are only two right (left) cosets, say H and H' (H and H''). Any element $a \in G$ not in H is necessarily in H' (H''), i.e., $H' = H''$. Hence H is normal.

(3) Classify all abelian groups of order 135.

Solution. If we apply the fundamental theorem of finitely generated abelian groups G with the additional assumption that $|G| < \infty$ we can have

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

such that $n_1 n_2 \cdots n_k = |G|$, $n_1 \geq 2$ and $n_{i+1} \mid n_i$. Since 135 has the prime factorisation $135 = 3^3 \times 5$. our only possible choices for $(n_1, \dots, n_k)$ are (135), $(45, 3)$, $(15, 3, 3)$ which gives

$$\mathbb{Z}/135\mathbb{Z}, \qquad \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \qquad \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Of course there are other ways to write this answer:

$$\mathbb{Z}/135\mathbb{Z} \cong \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

see question (1).

(4) Let R be a commutative ring with identity and let $I \subset R$ be an ideal. Show that I is a prime ideal if and only if R/I is an integral domain.

Solution. Let I be a prime ideal. To show that R/I is an ID we need to show that if $(a + I)(b + I) = I = 0_{R/I}$ then one of $a + I, b + I$ is I. We have $(a + I)(b + I) = ab + I$. This will be equal to I if $ab \in I$. Since I is a prime ideal, this implies that one of $a, b \in I$, so that one of $a + I, b + I$ is I as required.
For the converse, assume R/I is a domain. To show that I is a prime ideal we need to show that if $ab \in I$ then one of $a, b \in I$. But if $ab \in I$ then $(a + I)(b + I) = ab + I = I$. Since R/I is an ID this implies one of $a + I, b + I$ is I so that one of $a, b \in I$ as required.

(5) Let x be a nilpotent element of a ring with identity 1. Show that $1+x$ is a unit.

Solution. Since x is nilpotent only finitely many x^k for k a nonnegative integer are unequal to 0. Hence $1-x+x^2-x^3+\cdots$ is a well-defined element. We can check that

$$(1+x)(1-x+x^2-x^3+\cdots) = (1-x+x^2-x^3+\cdots)+(x-x^2+x^3-\cdots) = 1$$

so that $1+x$ is a unit.

(6) Determine all maximal and prime ideals of $\mathbb{C}[x]$. Justify your answer.

Solution. It is clear that $\langle x-a\rangle$ for $a \in \mathbb{C}$ is a maximal ideal of $\mathbb{C}[x]$ since $\mathbb{C}[x]/\langle x-a\rangle \cong \mathbb{C}$. (To see this you can define the homomorphism $f : \mathbb{C}[x] \to \mathbb{C}$ by $f(p(x)) = p(a)$ and appeal to the isomorphism theorem for rings.) Since $\mathbb{C}$ is a field it is simple and hence $\langle x-a\rangle$ is maximal. If a polynomial is reducible, i.e., $f(x) = g(x)h(x)$ then $\langle f(x)\rangle \subset \langle g(x)\rangle$ and $\langle f(x)\rangle \subset \langle h(x)\rangle$. By the fundamental theorem of algebra, polynomials over $\mathbb{C}$ of degree greater than 1 are all reducible and hence cannot be maximal. To complete the question we need something not covered this year: $\mathbb{C}[x]$ is a PID (principal ideal domain). An ID is a PID if every ideal is principal. A key result about PIDs is that fields and polynomial rings over fields are PIDs. (Also, a polynomial ring is a PID iff the coefficient ring is a field). Hence $\mathbb{C}[x]$ has no ideals that are not of the form $\langle f(x)\rangle$ and we are done.
Clearly, all of the maximal ideals are prime and $\langle f(x)\rangle$ with $f(x)$ a polynomial of degree greater than 1 is not prime. Since $\mathbb{C}[x]$ is a PID there is only one further ideal to consider, the zero ideal. Clearly this is also prime.

(7) Show that the number of conjugacy classes of nilpotent $n \times n$ matrices equals the number of partitions of n (Hint: use the Jordan Form).

Solution. Jordan form is not covered in 2016.

(8) Recall that $G = \mathrm{Gl}_n(\mathbb{R})$ acts on $\mathbb{R}^n$ as follows: a matrix $g \in G$ sends a vector $v \in V$ to the vector gv.
(i) Show that this action is transitive.
(ii) Determine $\mathrm{Stab}_G\big((1,0,\ldots,0)\big)$.
(iii) Now let

$$S = \{v \in \mathbb{R}^n \mid v^t v = 1\}.$$

Let $v = (1,0,\ldots,0)$. Give an example of $g \in G$ such that $gv \notin S$.
(iv) Show that $O(n)$ acts on S; that is, show that if $g \in O(n)$ and $s \in S$, then $gs \in S$.
(v) Show that $\mathrm{Stab}_{O(n)}\big((1,0,0,\ldots,0)\big)$ is isomorphic to $O(n-1)$.

Solution. Note: V in the above should be $\mathbb{R}^n$, $(1,0,\ldots,0)$ should be $(1,0,\ldots,0)^t$ since elements of $\mathbb{R}^n$ in this question should be viewed as column vectors, rather than row vectors. Also (i) should read "Show that this action is transitive on $\mathbb{R}^n\backslash\{\mathbf{0}\}$. Finally, in 2016 $\mathrm{Gl}_n(\mathbb{R})$ has been written as $\mathrm{GL}(n,\mathbb{R})$.
(i) Transitivity is not a notion explicitly covered in 2016. What it means is that there is only a single orbit under the action of $\mathrm{Gl}_n(\mathbb{R})$. In other words, every $v \in \mathbb{R}^n$ can be mapped to any $w \in \mathbb{R}^n$ under the action of G. This is not actually true, since the zero vector $\mathbf{0}$ forms its own orbit, hence the above correction. After excluding $\mathbf{0}$ transitivity should be clear. All we need to show is that every v is in the orbit of $(1,0,\ldots,0)^t$. Since not all components $v_1,\ldots,v_n$ of v are equal to 0 we can always complete the matrix

$$g = \begin{pmatrix} v_1 & * & \ldots & * \\ v_2 & * & \ldots & * \\ \vdots & & \vdots & * \\ v_n & * & \ldots & * \end{pmatrix}$$

so that $\det(g) \neq 0$, resulting in the required

$$g\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \begin{pmatrix}v_1\\v_2\\\vdots\\v_n\end{pmatrix}.$$

For example, if $v_1 \neq 0$ we can take

$$g = \begin{pmatrix} v_1 & 0 & 0 & \dots & 0 & 0 \\ v_2 & 1 & 0 & \dots & 0 & 0 \\ v_3 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & \ddots & & \\ v_{n-1} & 0 & 0 & \dots & 1 & 0 \\ v_n & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

and, more generally, if $v_i \neq 0$ we can take $g_{i,1} = v_i$

$$g_{i+1,2} = g_{i+2,3} = \cdots = g_{n,n-i+1} = g_{1,n-i+2} = g_{2,n-i+3} = \cdots = g_{i-1,n} = 1$$

and all other $g_{ij} = 0$ for $2 \leq j \leq n$.

(ii) Again this has not been explicitly covered this year. The stabilizer of a vector v refers to the subgroup of G that fixes v. If $v = (1, 0, \dots, 0)^t$ then we are looking for those $g \in G$ such that $g(1, 0, \dots, 0)^t = (1, 0, \dots, 0)^t$. These are the matrices whose first column is given by

$$\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}.$$

(iii) S is the unit $(n-1)$-sphere in $\mathbb{R}^n$. The given v corresponds to a point on S. Hence we are asked to find a g that changes the length of v. Simple examples are provided by the set of matrices

$$\{xI_{n\times n} : \ x \in \mathbb{R}^\times, x \neq \pm 1\}.$$

(iv) $O(n)$ stands for the group of orthogonal matrices, that is, $n \times n$ matrices of the form $gg^t = I_{n\times n}$. Orthogonal transformations leave lengths and angles in tact, if $\hat{v} = gv$ and $\hat{w} = gw$ and $(\cdot, \cdot)$ is the usual dot product in $\mathbb{R}^n$ then

$$(\hat{w}, \hat{v}) = (gw, gv) = (w, g^t gv) = (w, v).$$

The group $O(n)$ does not act transitively on $\mathbb{R}^n$ since vectors of different lengths cannot be transformed into each other. It does however act transitively on $(n-1)$-spheres, such as S, since any point on a sphere can be obtained from any other point by a rotation.

(iv) An $n \times n$ matrix whose first column is

$$\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$$

can only be orthogonal if its first row is $(1, 0, \dots, 0)$ (since $g^t g = I_{n\times n}$). Hence we must consider matrices g of the form

$$g = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

This is orthogonal iff the $(n-1) \times (n-1)$ submatrix consisting of the last $n-1$ rows and columns of g is an orthogonal matrix, so that

$$\mathrm{Stab}_{O(n)}\big((1, 0, 0, \dots, 0)^t\big) \cong O(n-1).$$