MATH3303: 2013 FINAL EXAM

(1) Write out all elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and compute the order of each elements.

Solution. For simplicity I will write 0 for $\bar{0}$ and 1 for $\bar{1}$. There are 16 matrices to consider but we need to rule out determinant 0. This rules out all 9 matrices with at least two zeros in a row/column and the all ones matrix. Hence we are left with the 6 elements:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad\begin{pmatrix}0&1\\1&0\end{pmatrix}\quad\begin{pmatrix}1&0\\1&1\end{pmatrix}\quad\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad\begin{pmatrix}1&1\\1&0\end{pmatrix}\quad\begin{pmatrix}0&1\\1&1\end{pmatrix}$$

The first matrix is the identity matrix (order 1), the next three matrices are involutions (order 2) and the last two matrices have order 3.

(2) Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Solution. Let $f : G \to G$ be the map in question, $f(g) = g^{-1}$. Let f to be a homomorphism, i.e., $f(g_1)f(g_2) = f(g_1g_2)$ for all $g_1, g_2 \in G$. From the definition of f this implies that

$$(g_1g_2)^{-1} = f(g_1g_2) = f(g_1)f(g_2) = g_1^{-1}g_2^{-1} = (g_2g_1)^{-1}.$$

Hence $g_1g_2 = g_2g_1$ for all $g_1, g_2 \in G$ so that G is abelian. Conversely, if G is abelian,

$$f(g_1g_2) = (g_1g_2)^{-1} = (g_2g_1)^{-1} = g_1^{-1}g_2^{-1} = f(g_1)f(g_2)$$

so that f is a homomorphism.

(3) (a) State Lagrange's Theorem.
(b) Use this theorem to show that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Solution. (a) Lagrange tells us that if G is a finite group with subgroup H then $|H|$ divides $|G|$. Morover, the ratio $|G|/|H|$, known as the index of H in G, counts the number of right (left) cosets of H in G.
(b) We know that $L := H \cap K$ is a subgroup of both H and K. Indeed, if $a, b \in L$ then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G this implies that also ab^{-1} is in H as well as K, i.e., then $ab^{-1} \in L$. Since H and K are finite, we also know that $|L|$ must divide both $|H|$ and $|K|$. Since H and K have no divisors in common other than 1, this implies that $|L| = 1$.

(4) Decide which of the following are subrings of $\mathbb{Q}$. Justify your answer.
(a) The set of all rational numbers with odd denominators (when the fraction is completely reduced)
(b) The set of all rational numbers with even denominators (again when the fraction is completely reduced)
(c) The set of nonnegative rational numbers.
(d) The set of squares of rational numbers
(e) The set of all rational numbers with odd numerators (when the fraction is completely reduced).

Solution. (a) This set is indeed a subring (integers are n are viewed as $n/1$). It contains 1, is an additive subgroup of $\mathbb{Q}$: $a/b \pm c/d = (ad \pm bc)/(bd)$ and if b, d are odd then so is bd (the right-handside may not be reduced but given that bd is odd, we cannot reduce it to an even demoninator) and it is closed under multiplication: $a/b \cdot c/d = ac/bd$ (again the right may not be reduced).
(b) This set is not a subring. It does not even contain a unit. Also, $1/6 + 1/6 = 1/3$ etc.
(c) Again this is not a subring. Only 0 has an additive inverse.
(d) Again this is not a subring: $1 + 1 = 2$.
(e) Addition is not closed: $1/1 + 1/1 = 2/1$, and 0 is missing.

(5) Determine all maximal and prime ideals of the polynomials ring $\mathbb{C}[x]$. 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.

(6) Let R be a commutative ring with identity, and let I be an ideal of R. Prove that I is maximal if and only if R/I is a field.

Solution. Let J be an ideal of R such that $I \subseteq J \subseteq R$. Then J/I is an ideal of R/I. If R/I is simple its only ideals are $0_{R/I}$ and R/I so that J must be one of $\{I, R\}$. Hence I is maximal. Conversely, we know that if K is an ideal of R/I then there exists an ideal $J \supset I$ of R such that $J/I = K$. If I is maximal the only possible J are $J = I$ and $J = R$ so that the only possible ideals K are $0_{R/I}$ and R/I. Hence R/I is simple.

(7) (a) Prove that every ideal in a Euclidean domain is principal.
(b) Exhibit an ideal in $\mathbb{Z}[x]$ which is not principal.

Solution. (a) Euclidean domains were not covered this year. For the record, Euclidean domains are domains that allow for a (Euclidean) division algorithm.
(b) We need an ideal generated by more than one polynomial. A simple choice is

$$I := \langle x, 2\rangle = \{2f(x) + xg(x),\ f(x), g(x) \in \mathbb{Z}[x]\}.$$

To see that I is not principal, assume by contradiction that the exists an $h(x) = c_k x^k + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ such that $I = \langle h(x)\rangle$. Clearly $2 \in I$ and $1 \notin I$. But

$$I = \{(c_k x^k + \cdots + c_1 x + c_0)f(x),\ f(x) \in \mathbb{Z}[x]\}$$

The only way to get 2 (and not 1) is to take $c_k = \cdots = c_1 = 0$ and $c_0 = 2$. But then

$$I = \{2f(x),\ f(x) \in \mathbb{Z}[x]\},$$

the set of even polynomials. This is a subset of $\langle x, 2\rangle$ since it does not contain the polynomial $x + 2$, for example. Hence we have a contradiction, and $\langle x, 2\rangle$ is not a principal ideal.

(8) Write the character table for S_3.

Solution. Character tables were not covered this year.