MATH3303: 2016 FINAL EXAM, (EXTENDED) SOLUTIONS

1. State the second isomorphism theorem for groups.

Solution. Let G be a group, $N \lhd G$ and $S \leq G$. Then (1) $N \cap S \lhd S$ and (2) $S/(N \cap S) \cong NS/N$.

2. Give the definition of a solvable group.

Solution. A group G is solvable if there exists a subnormal series

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_k = G$$

(for some integer $k \geq 1$) such that the quotients G_{i+1}/G_i are abelian for all $0 \leq i \leq k-1$.

3. State Wedderburn's theorem, and give the definition of all mathematical structures involved.

Solution. Wedderburn's theorems states that every finite division ring is a field. A division ring is a (non-zero) ring in which every non-zero element is a unit (a unit being an element with a multiplicative inverse). A finite division ring is a division ring with a finite number of elements. A field is a commutative division ring.

4. Let R be a ring.
(a) Under what conditions does R have a field of fractions, Frac(R)?
(b) Describe the full construction of Frac(R). You do not need to prove any of the (implicit) claims that make this construction work.
(c) Show that there is no smaller field in which R can be embedded.

Solution. (a) R must be an integral domain, that is, R must be commutative and, if $ab = ac$ and $a \neq 0$, then $b = c$.
(b) Let $T = R \times (R\backslash\{0\})$. Two elements (a, b) and (c, d) in T are said to be equivalent if $ad = bc$. This defines an equivalence relation on T. The fraction a/b is now defined as the equivalence class of T containing (a, b). The set of all such fractions can be given the structure of a field, Frac(R), by taking as addition and multiplication

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

(c) First we note that we can embed R in its field of fractions by identifying $a/1$ with a. The reason not all IDs are fields is that not all non-zero elements are necessarily units. Under the above identification, if $a \in R$ is a unit then the fraction $1/a \in R$ and, in fact, $1/a = a^{-1}$. Indeed, let a^{-1} be the inverse of a, then $1/a = a^{-1}/1$ since $1 \times 1 = a \times a^{-1}$. For the non-zero $a \in R$ that are *not* units, by adjoining R with the elements $1/a$ they become units. Hence no elements of

$$B = \{1/a : a \in R\backslash\{0\}\}$$

can be omitted from the field of fractions, either because it is already in R or it is required to turn a non-zero non-unit into a unit. But since R is closed under multiplication we then also need RB which is exactly the field of fractions constructed in (b).

5. Give the definition of a unique factorisation domain and explain the meaning of each of the notions used in the definition.

Solution. A UFD is an integral domain such that every non-zero non-unit can be 'uniquely' written as a product of irreducible elements. An irreducible element r of an ID is a non-zero non-unit such that $r = ab$ implies that one of a, b is a unit. The adverb 'uniquely' is to be understood as being unique (1) up to permutation of the irreducible factors (since a UFD is commutative it is clear that the order in which the irreducible elements are written is irrelevant) (2) up to units. That is, if a admits the

factorisation $a = r_1 r_2 \cdots r_k$ into irreducible elements r_i, then we may replace each r_i by an equivalent irreducible element s_i (the irreducibles r and s are equivalent if $r = su$ with u a unit) as long as the product of all the units involved in the rewriting is 1. For example $12 = 2 \times 2 \times 3 = (-2) \times 2 \times (-3)$ since $(-1) \times (-1) = 1$.

6. Let $f : G \to H$ be a homomorphism between groups. Prove that $\ker f \lhd G$. (Show both the subgroup and normality property.)

Solution. Let $K := \ker f$. Then $K = \{g \in G : f(g) = 1\}$ (where $1 = 1_H$). To prove that K is a subgroup we need to show that if $a, b \in K$ then $ab^{-1} \in K$. By the properties of homomorphisms,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1 \cdot 1 = 1$$

so that $ab^{-1} = 1$ as required. To prove that K is normal it suffices to show that all of the conjugates of k are in K, i.e., $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$. For $g \in g$ and $k \in K$ we have

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)1f(g)^{-1} = 1$$

so that $gkg^{-1} \in K$.

7. Let m, n, l be positive integers. For which values of m, n, l is it true that

$$(\mathbb{Z}/m\mathbb{Z})/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}$$

as an isomorphism of groups? Fully justify your answer.

Solution. Since $\mathbb{Z}/k\mathbb{Z}$ is a group of order k, we obviously must have $m/n = l$. Is this sufficient? By the third isomorphism theorem, if $N \lhd M \lhd G$ and $N \lhd G$, then (1) $M/N \lhd G/N$ and (2) $(G/N)/(M/N) \cong G/M$. Take $G = \mathbb{Z}$, $N = m\mathbb{Z}$ and $M = l\mathbb{Z}$. To meet the conditions of the theorem we only need $m \mid l$ which is certainly true if $m/n = l$. Then

$$(\mathbb{Z}/m\mathbb{Z})/(l\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/l\mathbb{Z}.$$

But $l\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ (the map $f : \mathbb{Z}/n\mathbb{Z} \to l\mathbb{Z}/ln\mathbb{Z} = l\mathbb{Z}/m\mathbb{Z}$ given by $f(k + n\mathbb{Z}) = lk + ln\mathbb{Z}$ clearly is an isomorphism) so that the only required condition is $m = nl$.

8. Show that all finite integral domains are fields.

Solution. Let R be an ID. That is, R is a commutative ring such that $ab = ac$ and $a \neq 0$ implies $b = c$. If R is finite, we may write $R = \{r_1, \ldots, r_n\}$. Now pick an arbitrary non-zero $r_i \in R$. Then $|r_i R| = |R|$ since $r_i r_k = r_i r_l$ for $1 \leq k \leq l \leq n$ implies that $r_k = r_l$ by the above property of IDs. Hence $r_i R$ contains the identity element of R, so that there is an $r_j \in R$ such that $r_i r_j = 1$. In other words, r_i is a unit. Hence $R^\times = R \backslash \{0\}$ so that R is a field (commutative ring in which all elements with the exception of the zero element are units).

9. Let $R = \mathbb{Q}[x]$ and $I = (x - m)\mathbb{Q}[x]$ for a fixed $m \in \mathbb{Z}$. Identify the quotient ring R/I. All your claims must be fully justified.

Solution. Since in R/I we may identify x with m this suggests that $R/I \cong \mathbb{Q}$. To prove this is indeed the case, we define the (ring) homomorphism $f : \mathbb{Q}[x] \to \mathbb{Q}$ by

$$f(p(x)) = p(m).$$

It is clear that f is surjective since the set of constant polynomials (over $\mathbb{Q}$) is a subset of $\mathbb{Q}[x]$ isomorphic to $\mathbb{Q}$, and the map f acts like the identity on this subset. The kernel of f is given by those polynomials that have a factor $x - m$, i.e., $\ker f = \langle x - m \rangle = (x - m)\mathbb{Q}[x] = I$. By the first isomorphism theorem for rings, $R/I \cong \mathbb{Q}$.

10. Show that an ideal I of a commutative ring R is prime if and only if R/I is an integral domain.

Solution. The elements of R/I are the cosets $r+I$ and the zero element of R/I is I.
$\Leftarrow$ Let I be prime. This implies that if $ab \in I$ for $a, b \in R$ then one of a, b is in I. Now assume that the product of two elements of R/I is zero, i.e.,

$$(r+I)(s+I) = I.$$

The left side may be expanded as $rs+I$ so that our assumption implies that $rs \in I$. By the primality of I this implies that one of r, s is in I, so that one of $r+I, s+I$ is equal to I (read, is zero in R/I). Hence R/I is an ID.
$\Rightarrow$ Let R/I be an ID. Pick $r, s \in R$ such that $rs \in I$. Then

$$(r+I)(s+I) = rs+I = I.$$

Since R/I is an ID this implies that one of $r+I, s+I$ is equal to I so that one of $r, s \in I$. Hence I is a prime ideal.

11. We say that a ring $R \neq 0$ is *local* if the set of non-units, J, is an ideal of R.
(a) Let R be a local ring. Show that R/J is a division ring.
(b) Let R be local. Show that if I is an ideal of R contained in J then R/I is local.
(c) Let I be an ideal of R such that all elements of I are nilpotent and such that R/I is a division ring. Show that R is local.

Solution. (a) Since R is local the set of non-units, J, is an ideal. The elements of the quotient ring R/J are the cosets $r+J$, with J the zero element and $1+J$ the identity element. If r is a non-unit, then $r \in J$ so that $r+J = J$. Hence all non-zero elements of R/J are of the form $r+J$ where r is a unit. We want to show that such elements themselves are units. But this is clear, because $r^{-1}+J$ is also a non-zero element of R/I (not necessarily distinct from $r+J$ but that is irrelevant) so that

$$(r+J)(r^{-1}+J) = rr^{-1}+J = 1+J$$

and

$$(r^{-1}+J)(r+J) = r^{-1}r+J = 1+J.$$

We thus conclude that all elements of R/J, except for J, are units so that R/J is a division ring.
(b) We need to show that the set of non-units in R/I, say K, is an ideal of R/I. Since $I \subseteq J$ we know that $J/I = \{j+I : j \in J\}$ is an ideal of R/I. We claim that the elements of J/I are non-units in R/I. Indeed, assume by contradiction that $j+I$ is a unit (for $j \in J$). Then there exists an $r \in R$ such that $(j+I)(r+I) = 1+I$. But $(j+I)(r+I) = jr+I \subseteq J$ since $jr \in J$ (absorbtion property) and $I \subseteq J$. This would thus imply that $1+I \subseteq J$ and hence that $1 \in J$, a contradiction. This proves that the the elements of J/I are non-units in R/I, so that $J/I \subseteq K$. But it is clear that $K \subseteq J/I$. Indeed, if $r+I \notin J/I = \{j+I : j \in J\}$ this means that $r \notin J$, i.e., that r is a unit. But if r is a unit then it has an inverse r^{-1} and $(r+I)(r^{-1}+I) = 1+I$ so that $r+I$ is a unit in R/I and hence not in K. We conclude that $K = J/I$. Since J/I, the set of non-units in R/I, is an ideal of R/I, this proves that R/I is local.
(c) Since R/I is a division ring, for all $r \in R$ such that $r \notin I$, $r+I$ is a unit. That is, for all $r \notin I$ there is an $s \in I$ such that

$$(r+I)(s+I) = rs+I = 1+I \quad \text{and} \quad (s+I)(r+I) = sr+I = 1+I.$$

The first of these equations implies that $rs \in 1+I$, i.e, $rs = 1+a$ with a a nilpotent element. Since $1+a$ is a unit (it has inverse $1-a+a^2-\cdots$) this implies that rs is a unit. Similarly, sr is a unit. But if rs and sr are both units then r and s themselves must be units. Indeed, since rs and sr are units there exists a t and q such that

$$trs = rst = 1 = qsr = srq.$$

But this implies that

$$st = 1(st) = (qsr)(st) = (qs)(rst) = (qs)1 = qs$$

so that $rst = 1 = qsr$ can be rewritten as $r(st) = 1 = (st)r$. Hence r is a unit (with inverse st). Although not needed, we note that in much the same way $tr = rq$ so that s is a unit with inverse tr. We conclude that any $r \notin I$ is a unit so that I contains all of the non-units of R. Hence $I = J$. Since I is an ideal this implies that J is an ideal, and hence that R is local.

An often made mistake was to conclude from $rs + I = 1 + I$ that $rs = 1$, whereas all it says is that $rs - 1 \in I$. For example, if $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$ then $1 + I$ is the set of all odd integers and so is $3 \times 5 + I$. But clearly $3 \times 5 \neq 1$.