McGill University - Fall 2018

Final Review - MATH 235

Ralph Sarkis

December 10, 2018

1 Groups

Exercise 1.1. Give non-isomorphic examples of:

i. A group of order 6.

ii. A non-commutative ring.

iii. An infinite field.

Solution.

i. C_6 and S_3.

ii. Matrices in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

iii. $\mathbb{Q}$ and $\mathbb{R}$

□

Exercise 1.2. True or false:

i. Let G and H be groups, $G \times H$ is abelian if and only if G and H are abelian.

ii. $\mathbb{Z}$ is an ideal of $\mathbb{Q}$.

iii. If R and S are field, then $R \times S$ is a field.

Solution.

i. True.

ii. False.

iii. False.

□

Exercise 1.3. Define the map $f : \mathbb{Z}_6 \to \mathbb{Z}_2$ by $f([a]) = [a]$. Show that this is well-defined and that it is a homomorphism. Find $\ker f$.

Solution. To show that it is well-defined, we need to show that if $a \equiv b \pmod 6$, then $a \equiv b \pmod 2$. This is true because if $a = b + 6k$, then $a = b + 2(3k)$. To see that f is a homomorphism, note that

$$f([a] + [b]) = f([a + b]) = [a + b] = [a] + [b] = f([a]) + f([b]),$$

and $f([0]) = [0]$.

It is easy to see that for $f([a])$ to be 0, we must have $a = 0, 2, 4$. $\square$

Exercise 1.4. Let $\mathbb{Q}$ be the additive group of rational numbers. The integers $\mathbb{Z}$ form a normal subgroup of $\mathbb{Q}$. Show that $\mathbb{Q}/\mathbb{Z}$ is an infinite group. Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order.

Solution. The additive group $\mathbb{Q}$ is commutative, thus every subgroup is normal. We need to find infinitely many elements that are not equivalent in $\mathbb{Q}/\mathbb{Z}$. Let $S = \{\frac{1}{n} \mid n \in \mathbb{N}\} \subseteq \mathbb{Q}/\mathbb{Z}$. If two elements of S are equivalent, then $\frac{1}{n} = \frac{1}{m} + z$ for some $z \in \mathbb{Z}$. If $z > 0$, then $\frac{1}{m} + z > 1 > \frac{1}{n}$. If $z < 0$, $\frac{1}{m} + z < 0 < \frac{1}{n}$. Thus, we have $z = 0$ which implies $m = n$. We conclude that there are infinitely many elements in $\mathbb{Q}/\mathbb{Z}$. $\square$

Exercise 1.5. Let p and q be distinct primes, and suppose that G is a group with $|G| = pq$. Suppose that $f : G \to H$ is an onto group homomorphism, but not one-to-one. Prove that H is abelian.

Solution. Since f is not injective, it has a nontrivial kernel $\ker f$. By Lagrange, $|\ker f| \mid pq = |G|$, and since p and q are primes, we have three options $|\ker f| \in \{p, q, pq\}$. Thus, $G/\ker f$ is a group of order p, q or 1 (it is always abelian). By the first isomorphism theorem $H \cong G/\ker f$, so H is always abelian. $\square$

Exercise 1.6. Let M and N be normal subgroups of G. Show that $M \cap N$ is also a normal subgroup of G.

Proof. For any $g \in G$, we want to show $g(M \cap N)g^{-1} = M \cap N$.

($\subseteq$) This follows from $gMg^{-1} \subseteq M$ and $gNg^{-1} \subseteq N$.

($\supseteq$) This follows from the fact that conjugation by any element g is an isomorphism. $\square$

Exercise 1.7. Let M and N be normal subgroups of G such that $G = \langle M, N \rangle$. Show that $G/(M \cap N) \cong G/M \times G/N$.

Solution. Let

$$\pi = \pi_A \times \pi_B : \langle A, B \rangle \to \frac{\langle A, B \rangle}{A} \times \frac{\langle A, B \rangle}{B} = g \mapsto (gA, gB),$$

we claim that π is surjective. Let (g_1A, g_2B) be in the R.H.S., with $g_1 = x_1x_2...x_n$ and $g_2 = y_1y_2...y_m$, with $x_i, y_i \in A \cup B$. Then using normality, we can write $g_1 = b_1a_1$ and $g_2 = a_2b_2$ for some $a_1, a_2 \in A, b_1, b_2 \in B$. So $(g_1A, g_2B) = (b_1a_1A, a_2b_2B) = (b_1A, a_2B)$ so the preimage of (g_1A, g_2B) under π is $g = b_1a_2$. Hence π is surjective.

We find the kernel of π. For an element $g \in G = \langle A, B \rangle$, we need $\pi(g) = (gA, gB)$ to be (A, B), that is $g \in A$ and $g \in B$ so $g \in A \cap B$. Hence $Ker(\pi) = A \cap B$. By the first isomorphism theorem, we get that $\frac{G}{\ker \pi} = \frac{G}{A \cap B} \simeq \frac{G}{A} \times \frac{G}{B} = \mathrm{Im}(\pi)$. $\square$

2 Rings

Exercise 2.1. Find all ring homomorphisms $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Solution. Note that f is defined by where it sends $(1,0)$ and $(0,1)$ and it must send $(1,1)$ to 1 and $(0,0)$ to 0. Furthermore, any $a, b \in \mathbb{Z}$ that satisfy $a + b = 1$ will yield a homomorphism f defined by $(1,0) \mapsto a$ and $(0,1) \mapsto b$ (it extends to $f(n,m) = na + mb$). $\square$

Exercise 2.2. Prove that $M_2(\mathbb{R})$ contains a subring isomorphic to $\mathbb{C}$.

Solution. Recall that $\mathbb{C}$ is generated by 1 and i, so we just need to find matrices A_1 and A_i such that $A_1 \cdot M = A_1$ for any matrices and $A_i^2 = -A_1$. We have

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A_i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

$\square$

Exercise 2.3. Which of these sets are ideals of the ring of functions from $[0,1]$ to $\mathbb{R}$.

i. The set of functions that are 0 on the rationals.

ii. The set of polynomial functions.

iii. The set of functions with a finite number of zeros.

Solution.

i. This is an ideal because for any f, g in the set and h in the ring, for any $x \in \mathbb{Q} \cap [0,1]$, $(f + gh)(x) = f(x) + g(x)h(x) = 0 + 0h(x) = 0$.

ii. This is not an ideal because multiplying by a weird function will not always yield a polynomial.

iii. This is not an ideal, again because it is not closed under multiplication by elements of the ring.

$\square$

Exercise 2.4. Let R_1 and R_2 be rings, show that the ideals of $R_1 \times R_2$ are of the form $I_1 \times I_2$ where $I_1 \lhd R_1$, $I_2 \lhd R_2$. Find all ideals of $k \times k$ when k is a field.

Solution. Let $J \lhd R$ and define

$$I_1 = \{r_1 \mid \exists r_2 \in R_2, (r_1, r_2) \in J\} \qquad I_2 = \{r_2 \mid \exists r_1 \in R_1, (r_1, r_2) \in J\}.$$

We claim that $J = I_1 \times I_2$ and that $I_1 \lhd R_1$ and $I_2 \lhd R_2$.

First, for any $r_1 \in I_1$ and $r_2 \in I_2$, we have $r \in R_1$ and $s \in R_2$ such that $(r_1, s), (r, r_2) \in J$, then we have

$$(r_1, r_2) = (r_1, s)(1,0) + (r, r_2)(1,0) \in J.$$

Hence, $J = I_1 \times I_2$. Since $(0,0) \in J$, we have $0 \in R_1, R_2$, thus $I_1 \times 0 \lhd J$. We will show that $I_1 \lhd R_1$ and the symmetric proof will work for I_2. Let $a, b \in I_1$ and $r \in R_1$, then $a + rb \in I_1$ because $(a,0) + (r,0)(b,0) = (a + rb, 0) \in J$. It follows that I_1 is an ideal.

For the second part, recall that ideals of a field are either 0 or the whole field. Thus the ideals are 0×0, $0 \times k$, $k \times 0$ and $k \times k$. □

Exercise 2.5. Let R_1 and R_2 be two commutative rings, show that the prime ideals of $R_1 \times R_2$ are of the form $I_1 \times R_2$ or $R_1 \times I_2$ where $I_1 \lhd R_1$, $I_2 \lhd R_2$. What are the prime ideals of $k \times k$ when k is a field.

Solution. Let $I \lhd R_1 \times R_2$, then if $(a,b), (c,d) \in I$, then $I = I_1 \times I_2$ for two ideals $I_1 \lhd R_1$ and $I_2 \lhd R_2$ (from last exercise).

Suppose that I_1 is a prime ideal and $I_2 = R_2$ (the symmetric case is the same argument), then $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \in I$ means $a_1 a_2 \in I$, so either $a_1 \in I_1$ or $a_2 \in I_1$ leading respectively to $(a_1, b_1) \in I$ or $(a_2, b_2) \in I$. We conclude that $I_1 \times R_2$ is a prime ideal of $R_1 \times R_2$ when I_1 is a prime ideal of R_1.

Conversely, if $I = I_1 \times I_2$ is a primes ideal and $a_1 a_2 \in I$, then $(a_1, 0)(a_2, 0) = (a_1 a_2, 0) \in I$, so either $(a_1, 0) \in I$ or $(a_2, 0) \in I$ leading respectively to $a_1 \in I_1$ or $a_2 \in I_1$. We conclude (after a symmetric argument) that I_1 and I_2 are either prime ideals or the whole ring.

We know that we cannot have $I_1 = R_1$ and $I_2 = R_2$, otherwise I is not prime, but it remains the case where both are proper ideals. This case leads to I being not prime because $(a, 0)(0, b) = (0, 0) \in I$ for any $a \notin I_1$ and $b \notin I_2$.

For the second part, the only ideals are $k \times 0$ and $0 \times k$. □

Exercise 2.6. Show that (x, y) is not a principal ideal of $\mathbb{Q}[x, y]$.

Solution. Assume that $(x, y) = (p)$ for some $p \in \mathbb{Q}[x, y]$, then $x = q_1 p$ and $y = q_2 p$. Since q_1, q_2 cannot have negative degrees in x and y, p must have degree 0 in x and y. Therefore, x must be a constant. Moreover, $p \neq 0$ or $q_1 p$ would be 0 as well, but there are no non-zero constant in (x, y), so we get a contradiction. □

3 Polynomial Rings

Exercise 3.1. Find all roots of $p = 3x^3 + 11x^2 + 5x - 3$.

Solution. Use rational root theorem to find $\frac{1}{3}, -3, 1$. □

Exercise 3.2. Let $f = x^5 + 5x + 5$ and $g = x^5 + 25x + 25$. Which of these polynomials is irreducible in $\mathbb{Z}[x]$.

Solution. Both are irreducible. For the first one, we can use Eisenstein. For the second one, we cannot conclude with Eisenstein but rational root theorem will show irreducibility in $\mathbb{Z}[x]$. □

Exercise 3.3. Factorize $p = x^6 + x^2 + x$ in $\mathbb{Z}_3[x]$.

Solution. We can easily see that x is a factor yielding $p = x(x^5 + x + 1)$. We can now easily check for the roots because we are in $\mathbb{Z}_3$. We have $1^5 + 1 + 1 = 3 \equiv 0 \pmod 3$ and $2^5 + 2 + 1 = 35 \equiv 2 \pmod 3$. We can divide by $x - 1$, to obtain $p = x(x - 1)(x^4 + x^3 + x^2 + x - 1)$. We check for roots again: $1^4 + 1^3 + 1^2 + 1 - 1 = 3 \equiv 0$ and $2^4 + 2^3 + 2^2 + 2 - 1 = 29 \equiv 2 \pmod 3$. We can divide by $x - 1$ again yielding $p = x(x-1)(x-1)(x^3 - x^2 + 1)$.

Recall that for polynomials of degree 2 or 3, reducibility implies existence of a root because one factor will have to be of degree 1. We can check that $x^3 - x^2 + 1$ has no roots in $\mathbb{Z}_3$ and conclude that we got the unique factorization. □

Exercise 3.4. Show that there exists a monic quadratic irreducible polynomial in $\mathbb{Z}_p[x]$ for any prime p.

Solution. We will use a counting argument. Any monic quadratic reducible polynomial has the form $(x - a)(x - b)$ where $a, b \in \mathbb{Z}_p$ and the order is irrelevant, so we get $\binom{p}{2} + p$ such polynomials.

Any monic quadratic polynomial has the form $x^2 + ax + b$ where $a, b \in \mathbb{Z}_p$, but now the order is relevant. So, we get p^2 such polynomials. We can now compare:

$$p^2 - \binom{p}{2} + p = p^2 - p - \frac{p^2 - p}{2} = \frac{p^2 - p}{2} \geq 1.$$

□

Exercise 3.5. Show that $p(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$ is irreducible in $\mathbb{Z}[x]$.

Solution. We will instead look at $q(x) = p(x - 1) = x^4 - 2x - 1$. Note that for $x = 2$, we have $q(2) = 11$ and for $x \geq 2$, we have $q'(x) = 4x^3 - 2 > 0$. Also, for $x = -2$, we have $q(-2) = 19$ and for $x \leq -2$, $q'(x) = 4x^3 - 2 < 0$. Thus, no roots can be outside $(-2, 2)$. We check that $0, -1$ and 1 are not roots and conclude that this polynomial is irreducible. □

Exercise 3.6. Let n be an integer. Show that if there exists $a, b \not\equiv 0 \pmod n$ such that $a^2 + b^2 \equiv 1 \pmod n$ and $ab \equiv 0 \pmod n$, then x is reducible in $\mathbb{Z}_n[x]$. Show that this cannot happen if n is prime.

Solution. For the first part, we note that

$$(ax + b)(bx + a) = abx + (a^2 + b^2)x + ab = x.$$

For the second part, no such a and b exist because if $n \mid ab$ and n is primes, we have that either $n \mid a$ or $n \mid b$. □

Exercise 3.7. Find four fields in which $p(x) = x^3 + x + 1$ has a root and with no injective homomorphism between each field.

Solution. Our first field is $\mathbb{C}$. It is algebraically closed, so any polynomials (hence p) has a root.

Next, we try with finite fields. Note that p is irreducible in $\mathbb{Z}_2$ since it has no roots. However, this lets us create a new field $\mathbb{Z}_2[x]/(p(x))$ with $2^3 = 8$ elements and in which p has a root (it is x).

Our third field is $\mathbb{Z}_3$, in which $p(1) \equiv 0$.

In $\mathbb{Z}_5$, p has no roots, so it is irreducible. Thus, we can use the same construction as before to get $\mathbb{Z}_5[x]/(p(x))$ which is a field with $5^3 = 125$ elements.

To see that there is not injective homomorphisms, note that each field we constructed has a different characteristic (minimum n such that $n \cdot 1 = 1 + \overset{n}{\cdots} + 1 = 0$, for $\mathbb{C}$, the characteristic is infinite) and the characteristics of the finite fields are coprime. $\square$