MA 741: Algebra I / Fall 2020
Homework assignment #4
Due Thursday, October 15, 2020 or soon thereafer

Clean copy

Thanks to Alanna, Benedikt, Duncan, and Yaron for pointing out typos, inconsistencies, and trouble points on this set.

When you turn in your solutions, please do not forget to identify yourself, this course, and the number of the HW set in the document name. Please also indicate if you worked with anyone else.

Edit 10/8/20: To turn in your work, email your well-titled document to `buma741fall2020@gmail.com` with "HW 4" in the subject line.

(0) Read and review

(a) Free groups, presentations: DF pp. 25–27 and section 6.3. Try DF exercise 1.2.18 on p.28.

(b) Rings: DF sections 7.1, 7.2, 7.3, but recall that unlike DF we assume that all rings have a multiplicative identity. If it's helpful, Keith Conrad has notes notes on ring definitions to replace DF's:
https://kconrad.math.uconn.edu/blurbs/ringtheory/ringdefs.pdf.

(1) **Quaternion group: presentation, automorphisms:** DF 6.3.7 and 6.3.9 on pp. 220–21.

(2) **Left and right units:** An element a of a ring A is a *left unit* (or *right invertible*) if there exists $b \in A$ with $ab = 1$. Such a b is a *right inverse* for a. Similarly, a is a *right unit* (or *left invertible*) if there exists $c \in A$ with $ca = 1$. Such a c is a *left inverse* for a.

(a) Show that $a \in A$ is a left unit if and only if the multiplication-by-a-on-the-left map $x \mapsto ax$ is surjective on A. Similarly, show that $a \in A$ is a right unit if and only if multiplication by a on the right is surjective on A.

(b) If $a \in A$ is both a left unit and a right unit (a is a *two-sided unit*, or simply *unit*), show that its left inverse is unique and agrees with its right inverse, which is also unique.

(c) Give an example of a ring that has a left unit which is not a right unit. Give an example of a ring that has a right unit which is not a left unit. Can you find multiple one-sided inverses for each? (If you get stuck, ask for a hint.)

(d) Now let A be an arbitrary ring again. Let $a \in A$ be a left unit with right inverse b. Show that for every $n \geq 0$, the element

$$b_n := b + (1 - ba)a^n$$

is a right inverse for a.

(e) Show that the following are equivalent for a left unit a:

(i) a is not a two-sided unit;

(ii) a has at least two distinct right inverses;

(iii) a has infinitely many distinct right inverses.

(*Hint*: Show that if $b_n = b_m$ for $n \neq m$, then a has a left inverse.) This is a theorem of Kaplansky; the constructive argument suggested here is due to Jacobson.

(3) **Zero divisors:** An element a of a ring A is a *left zero divisor* if there exists a nonzero $b \in A$ with $ab = 0$. It is a *right zero divisor* if there exists a nonzero $b \in A$ with $ba = 0$. A *zero divisor* is either a left or a right zero divisor. (Note the difference with the definitions in (2): being a unit is "good", so a unit has to be two-sided, whereas being a zero divisor is "bad", so one-sidedness is enough to qualify.)

(a) Show that $a \in A$ is a left zero divisor if and only if left multiplication by a is *not* an injective map $A \stackrel{x \mapsto ax}{\longrightarrow} A$. Similarly, $a \in A$ is a right zero divisor if and only if right multiplication by a is not injective.

(b) If $a \in A$ is a left unit (see (2)), then a is not a right zero divisor. Similarly, if $a \in A$ is a right unit, then a is not a left zero divisor.

(c) If $a \in A$ is not a left zero divisor, then a is *left cancellable*: for $b, c \in A$, we have $ab = ac$ implies $b = c$. State and prove the analogous right-side statement.

(d) If $a \in A$ is a left unit with more than one right inverse, show that a is a left zero divisor. Analogous statement on the other side?

(e) What are the zero divisors of $\mathbb{Z}/n\mathbb{Z}$? Here $n \in \mathbb{Z}^+$.

A nonzero commutative ring with no nonzero zero divisors is called an *integral domain*. If A is an integral domain, then any nonzero $a \in A$ is cancellable.

(4) **Products of rings**

(a) Let I be an indexing set, and R_i, $i \in I$, a collection of rings. Show that the set product $R := \prod_{i \in I} R_i$ with componentwise operations satisfies the universal property for products of rings: R is a ring equipped with maps $\pi_i : R \longrightarrow R_i$ for each i, and given any ring S with maps $f_i : S \longrightarrow R_i$ for each i, there's a unique map $\beta : S \longrightarrow R$ factoring each f_i: that is, satisfying $f_i = \pi_i \circ \beta$ for each i.

(b) Now let R_1 and R_2 be two rings, and for $i = 1, 2$, let $\pi_i : R_1 \times R_2 \longrightarrow R_i$ be the projection map guaranteed by (4a). Are there ring homomorphisms $\iota_i : R_i \longrightarrow R_1 \times R_2$ with ι_i a section (right inverse) of π_i? Explain.

(c) Continuing with $I = \{1, 2\}$, does $R_1 \times R_2$ satisfy the universal property for rings that is dual to the product property? (See HW #1 5b; replace every instance of "group" with "ring".) If yes, prove it. If no, explain. What kind of ring would satisfy such a property for $R_1 = \mathbb{Z}[x]$ and $R_2 = \mathbb{Z}[y]$ in the world of *commutative* rings?

(5) **Characteristic of a ring:** As pointed out in class, there's a unique ring homomorphism

$$\mathbb{Z} \longrightarrow R$$

for any ring R. The nonnegative generator n of the kernel $n\mathbb{Z}$ of this homomorphism is called the *characteristic* of R.

(a) Determine the characteristic of the rings (i) $\mathbb{Q}$, (ii) $\mathbb{Z}[x]$, (iii) $\mathbb{Z}/n\mathbb{Z}$, (iv) $\mathbb{Z}/n\mathbb{Z}[x]$, (v) $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$, (vi) $A = \{(a, b) : a \equiv b \pmod{n}\} \subseteq \mathbb{Z} \times \mathbb{Z}$, (vii) $\prod_{p \text{ prime}} \mathbb{Z}/p\mathbb{Z}$. Is there a ring of characteristic 1?

(b) Let p be prime and R a commutative ring of characteristic p. Prove that for all $a, b \in R$ we have $(a + b)^p = a^p + b^p$. Must this still hold if R is not commutative?

(c) Show that the characteristic of an integral domain (see (3)) is either 0 or a prime number p.

(6) (a) Construct a field with 4 elements by giving an addition and multiplication table. Remember that two of the elements have to be 0 and 1. Explain! How many nonisomorphic such fields can you construct?

(b) Show that the ring $\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$ is a field. How many elements does it have? Compare to your answers from part (a).

(7) **Monomorphisms and epimorphisms:** A map $\alpha : A \longrightarrow B$ of groups (respectively, abelian groups, rings, etc.) is said to be *monic* or a *monomorphism* if it is *left cancellable*: that is, whenever $f, g : C \longrightarrow A$ are two maps from another group (respectively, abelian group, ring, etc.) C to A

$$C \underset{g}{\overset{f}{\rightrightarrows}} A \xrightarrow{\alpha} B$$

then $\alpha \circ f = \alpha \circ g$ implies $f = g$.

(a) Show that a homomorphism of groups is injective if and only if it is monic.

A monomorphism therefore captures some property of being injective without any reference to elements; that's one of the goals of category theory.

Dually (that is, reversing all arrows), a map $\beta : B \longrightarrow A$ is said to be *epi* or an *epimorphism* if it is *right cancellable*: that is, whenever $f, g : A \longrightarrow C$ are two maps

$$B \xrightarrow{\beta} A \underset{g}{\overset{f}{\rightrightarrows}} C$$

then $f \circ \beta = g \circ \beta$ implies $f = g$.

(b) (i) Show that a surjective homomorphism of groups is epi.

(ii) Show that a epimorphism of abelian groups is always surjective.

(iii) Let $G = S_3$ and $H = \{e, (12)\} \subset G$. Show that the inclusion $H \hookrightarrow G$ is not an epimorphism.

More generally, it's true that a homomorphism of groups is surjective if and only if it is epi. See (10) below for hints and references.

Now consider commutative rings.

(c) Show that a homomorphism of commutative rings is injective if and only if it is monic.

(d) Convince yourself that your argument from (7(b)ii) still works to show that a surjection is an epimorphism. But show that the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is epi without being surjective.

Think about the following problems, but you do not need to turn anything in.

(8) Let A be a commutative ring, In class, we defined $A[\sqrt{d}]$ for $A = \mathbb{Z}, \mathbb{Q}$ as a ring structure on the abelian group $A \times A$, where we write an element (a, b) as $a + b\sqrt{d}$. Multiplication is defined by the fact that $1 + 0\sqrt{d}$ is the multiplicative identity and $(0 + 1\sqrt{d})^2 = d$ (convince yourself that these two facts plus the ring properties really do define a ring structure on $A[\sqrt{d}]$. We saw in class that if $d \in \mathbb{Z}$ is squarefree then $\mathbb{Q}[\sqrt{d}]$ is a field, isomorphic to the subfield $\mathbb{Q}(\sqrt{d})$ of $\mathbb{C}$.

(a) Suppose $d = e^2$ is the square of positive integer. Show that the map

$$\mathbb{Q}[\sqrt{d}] \longrightarrow \mathbb{Q} \times \mathbb{Q}$$

defined by

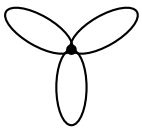
$$a + b\sqrt{d} \mapsto (a + be, a - be)$$

is an isomorphism of rings.

(b) Still supposing that $d = e^2$ for some $e \in \mathbb{Z}^+$, identify $\mathbb{Z}[\sqrt{d}]$ with a subring of $\mathbb{Z} \times \mathbb{Z}$. Explain.

(c) Now take any nonzero $d \in \mathbb{Z}$. Describe $\mathbb{R}[\sqrt{d}]$ as simply as possible.

(9) The free group $F_n := F(\{s_1, \ldots, s_n\})$ appears in algebraic topology as the fundamental group of a bouquet of n circles. Call this bouquet B_n. Below, an image of B_3.



Suppose $G \subset F_n$ is a subgroup of finite index d. The Nelson-Schreier theorem tells us that G is also free. Explain the *Schreier index formula*: $G \cong F_r$, where $r = 1 + d(n - 1)$.

(Let X be the covering space of B_n corresponding to G, so that $G = \pi_1(X)$. Then X is contractible to a bouquet of r circles. Now use the Euler characteristic multiplicative formula for covering spaces (for example, exercise 2.2.22 in Hatcher's Algebraic Topology) to conclude that $d(1 - n) = 1 - r$.)

(10) Show that an epimorphism of groups is surjective.

(It suffices to show that if $H \subsetneq G$ is a proper subgroup of a group G, then there exists a group K and distinct maps $f, g : G \longrightarrow K$ with $f|_H = g|_H$. Let $G/H^* := G/H \cup \{*\}$, the set of left cosets of H in G augmented by an additional element $*$. Consider the left translation action of G on G/H, and the same but with the elements H and $*$ of G/H^* switched, as permutations of G/H^*.

This statement was originally proved by Schreier, but the argument suggested here is due to Linderholm[(i)]. See also Arturo Magidin's posts here and here.)

[(i)] BU sign-in required: https://www-jstor-org.ezproxy.bu.edu/stable/pdf/2317336.pdf.