MA 741: Algebra I / Fall 2020
Homework assignment #6
Due Wednesday, November 4

To turn in your work, please email your well-titled document (title should identify you, this course, and the HW set number) to `buma741fall2020@gmail.com` with "HW 6" in the subject line. Please indicate with whom you worked on the problem set.

(1) Consider the rings $\mathbb{F}_3[x]/(x^2+1)$, $\mathbb{F}_3[y]/(y^2+2y+1)$, $\mathbb{F}_3[z]/(z^2+2z+2)$, $\mathbb{F}_3[t]/(t^2+2)$. Which, if any, are fields? Which, if any, have zero divisors? Which, if any, have nilpotent elements? Classify them up to isomorphism: for each pair either construct an explicit isomorphism or explain why none exists. Are there any additional ring homomorphisms between them?

(2) Recall that an element α in a commutative ring A is a *root* of a polynomial $f(x) \in A[x]$ if $f(\alpha) = 0$. In class we showed that α is a root of $f \iff (x - \alpha) \mid f$.

(a) Let K be a field. Show that a polynomial of degree n in $K[x]$ can have no more than n distinct roots in K.

(b) Give an example of a ring A and a polynomial in $A[x]$ of degree $n \geq 1$ with more than n roots in A. Are there any such examples when A is a domain?

(c) Let K be a field again, and $G \subseteq K^\times$ be a finite group. Show that G is cyclic. (*Hint*: Let m be the maximal (multiplicative) order of any element of G, and consider polynomial $x^m - 1 \in K[x]$.)

(d) Let F be a finite field. Show that the underlying additive group structure of F must be $(\mathbb{Z}/p\mathbb{Z})^n$ for some prime p and some $n \geq 1$. Show that $F \cong \mathbb{F}_p[x]/(f(x))$ for some prime p and irreducible polynomial $f(x)$.

(3) **Rings of fractions** (Aluffi exercise V.4.7): Let A be a commutative ring. Recall that a subset $S \subseteq A$ is called a *multiplicatively closed* subset if it's a submonoid of $(A, \cdot)$: that is, $1 \in S$ and $s, t \in S \implies st \in S$.

Let $S \subseteq A$ be a multiplicatively closed subset. Define a relation on $A \times S$ by

$$(a, s) \sim (a', s') \text{ if there exists } t \in S \text{ such that } t(as' - a's) = 0.$$

(a) Show that $\sim$ is an equivalence relation.

(b) Is the relation $\overset{*}{\sim}$ on $A \times S$ given by $(a, s) \overset{*}{\sim} (a', s')$ if $as' = a's$ an equivalence relation as well? Explain.

(c) Denote by $\frac{a}{s}$ the equivalence class of (a, s) under $\sim$. Show that the binary operations

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} \qquad \text{and} \qquad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

are well defined.

Write $S^{-1}A$ for the set of equivalence classes $(A\times S)/\sim$. Convince yourself that $S^{-1}A$ is a commutative ring, and that the map $\ell : a \mapsto \frac{a}{1}$ defines a ring homomorphism $\ell : A \longrightarrow S^{-1}A$ with $\ell(S) \subset (S^{-1}A)^\times$.

(d) Show that $S^{-1}A$ satisfies the following universal property: if $f : A \longrightarrow B$ is a ring homomorphism from A to a commutative ring B with $f(S) \subset B^\times$, there is a unique ring homomorphism $\alpha : S^{-1}A \longrightarrow B$ factoring f: that is, satisfying $f = \alpha \circ \ell$.

(e) Show that $S^{-1}A$ is the zero ring if and only if $0 \in S$. If A is a domain and $0 \notin S$, show that $S^{-1}A$ is a domain.

(4) **Maps on** Spec**s induced by a ring homomorphism**: Let $\varphi : A \longrightarrow B$ be a homomorphism of commutative rings. If $\mathfrak{b}$ is an ideal of B, convince yourself that $\varphi^{-1}(\mathfrak{b})$ is an ideal of A. The ideal $\varphi^{-1}(\mathfrak{b})$ is sometimes denoted $\mathfrak{b}^{\mathrm{c}}$, the *contraction* of $\mathfrak{b}$. If $\mathfrak{a}$ is an ideal of A, write $\mathfrak{a}^{\mathrm{e}}$ for the ideal of B generated by $\varphi(\mathfrak{a})$: this is the *extension* of $\mathfrak{a}$.

(a) If $\mathfrak{b}$ is a prime ideal of B, show that $\mathfrak{b}^{\mathrm{c}}$ is a prime ideal of A. If $\mathfrak{b}$ is maximal in B, must $\mathfrak{b}^{\mathrm{c}}$ be maximal? Explain: that is, prove this or give a counterexample.

Let $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. From (4a), we see that φ induces a map $\varphi^* : Y \longrightarrow X$ defined by $\varphi^*(\mathfrak{q}) := \mathfrak{q}^{\mathrm{c}}$ for a prime ideal $\mathfrak{q} \subset B$.

(See problem 5 on HW #5 for the definition of $\operatorname{Spec} A$, its subset $V(\mathfrak{a})$ for an ideal $\mathfrak{a} \subseteq A$, and its Zariski topology.)

(b) If $\mathfrak{a}$ is an ideal of A, show that $(\varphi^*)^{-1}\big(V(\mathfrak{a})\big) = V(\mathfrak{a}^{\mathrm{e}})$. Conclude that φ^* is a continuous map of topological spaces.

(c) If φ is surjective, show that φ^* is a homeomorphism of Y onto the closed subset $V(\ker\varphi)$ of X. (That is, show that φ^* is one-to-one with image $V(\ker\varphi)$, and closed subsets of Y map to closed subsets of $V(\ker\varphi)$.)

(d) If $Z \subseteq X$ and $\mathfrak{a}$ is an ideal of A, show that $Z \subseteq V(\mathfrak{a})$ if and only if $\mathfrak{a} \subseteq \bigcap_{\mathfrak{p}\in Z} \mathfrak{p}$. Conclude that

$$\overline{Z} = V\Big(\bigcap_{\mathfrak{p}\in Z} \mathfrak{p}\Big).$$

Here $\overline{Z}$ is the *closure* of Z in X, that is, the intersection of all the closed subsets containing Z.

(e) If $\mathfrak{b}$ is an ideal of B, show that $\overline{\varphi^*\big(V(\mathfrak{b})\big)} = V(\mathfrak{b}^{\mathrm{c}})$.
Conclude that if φ is injective, then $\varphi^*(Y)$ is *dense* in X: that is, $\overline{\varphi^*(Y)} = X$.

This is a variation on part of AM exercise 1.21.

(5) **More rings of fractions:** Continue the notation of (3): A is a commutative ring, $S \subset A$ is a multiplicatively closed subset, and $\ell : A \longrightarrow S^{-1}A$ is the map $a \mapsto \frac{a}{1}$.

(a) If $\mathfrak{a}$ is an ideal of A with $\mathfrak{a} \cap S = \varnothing$, show that $\mathfrak{a}^{\mathrm{e}}$ is a proper ideal of $S^{-1}A$. Note that $\mathfrak{a}^{\mathrm{e}}$ is the set of equivalence classes of fractions of the form $\frac{a}{s}$ for $a \in \mathfrak{a}$ and $s \in S$.

(b) Conversely, if $\mathfrak{b}$ is a proper ideal of $S^{-1}A$, show that $\mathfrak{b}^{\mathrm{c}} \cap S = \varnothing$.

(c) Show that extension and contraction along ℓ gives a one-to-one correspondence between prime ideals $\mathfrak{p}$ of A with $\mathfrak{p} \cap S = \varnothing$ and prime ideals of $S^{-1}A$.

If $\mathfrak{p} \subset A$ is a prime ideal, verify that $S = A - \mathfrak{p}$ is multiplicatively closed. In this case the ring of fractions $S^{-1}A$ is the *localization of A at $\mathfrak{p}$*, often denoted $A_{\mathfrak{p}}$.

(d) Describe the localization $\mathbb{Z}_{(p)}$ for a prime number p. What are its prime ideals? What is the fraction field of $\mathbb{Z}_{(p)}$?

(e) Same questions for $S^{-1}\mathbb{Z}$ for $S = \{p^n : n \geq 0\}$. Again, p is a prime.

(6) **Extending characters from subgroups:** Let H be a normal subgroup of a group G and $\psi : H \longrightarrow \mathbb{C}^\times$ is a character. For $g \in G$, consider the map

$$ {}^g\psi : H \longrightarrow \mathbb{C}^\times $$

given by ${}^g\psi(x) = \psi(g^{-1}xg)$.

(a) Show that ${}^g\psi$ is a character of H, and only depends on the image of g in G/H.

(b) Suppose that G/H is a finite cyclic group. Show that ψ extends to a character of G if and only if $\psi = {}^g\psi$ for all $g \in G$.

(*Hint*: Suppose G/H has order n and is generated by the image of $x \in G$. Let $\zeta \in \mathbb{C}^\times$ be any n^{th} root of $\psi(x^n)$. Define $\widetilde{\psi} : G \longrightarrow \mathbb{C}^\times$ by $\widetilde{\psi}(x^i h) = z^i \psi(h)$ for any $h \in H$ and $0 \leq i < n$. When is $\widetilde{\psi}$ a character extending ψ?)

Now let G be a finite abelian group.

(c) If $H \subseteq G$ is a subgroup, show that any complex character of H extends to a character of G, in $(G : H)$ different ways.

(d) If $g \in G$ is not the identity element, show that there exists a character $\chi \in \hat{G}$ with $\chi(g) \neq 1$.

(e) Let $\hat{\hat{G}}$, the "double dual" of G, be the set of complex characters of $\hat{G}$. Show that the map $\mathrm{ev} : G \longrightarrow \hat{\hat{G}}$ sending g to the evaluation-at-g character $\mathrm{ev}_g : \hat{G} \longrightarrow \mathbb{C}^\times$, which maps $\chi \in \hat{G}$ to $\mathrm{ev}_g(\chi) := \chi(g)$, is an isomorphism of finite abelian groups.

Unlike the isomorphism between G and $\hat{G}$ that you constructed in 5c of HW #3, the isomorphism $\mathrm{ev} : G \longrightarrow \hat{\hat{G}}$ here is *canonical*: it does not depend on arbitrary choices!