Homework #1

Plan for next week: Existence of maximal ideal (§ 7.4), Rings of Fractions (§ 7.5), Euclidean Domains (§ 8.1), start PIDs (§ 8.2).

Problems, to be submitted by Thursday, September 3rd

1. Let G be a group.

(a) Define $\varphi : G \to G$ by $\varphi(g) = g^2$. Prove that φ is a homomorphism if and only if G is abelian.
(b) Assume that $x^2 = 1$ for any $x \in G$. Prove that G is abelian.

2. A group G is called *finitely generated* if there exists a finite subset S of G such that $\langle S \rangle = G$.

(a) Prove that every finite group is finitely generated.
(b) Let $\mathbb{Q}$ be the group of rational numbers with addition. Prove that $\mathbb{Q}$ is not finitely generated. **Hint:** If G is an abelian group written additively and $S = \{s_1, \ldots, s_n\}$ is a finite subset of G, what is the general form of an element of the subgroup $\langle S \rangle$?
(c) Prove that any finitely generated subgroup of $\mathbb{Q}$ is cyclic.

3. Prove that an element $\bar{a} \in \mathbb{Z}_n$ is invertible if and only if $gcd(a, n) = 1$ where *gcd* is the greatest common divisor. You may use any standard theorem about integers (e.g. unique factorization), but do not use any theorems about $\mathbb{Z}_n$. Give a detailed argument.

4. Let R and S be rings with 1, and let $\varphi : R \to S$ be a ring homomorphism. Assume that S is a domain and φ is not identically zero. Prove that $\varphi(1_R) = 1_S$.

5.

(a) Problem 7.3.34 in Dummit and Foote (DF). Note: in all exercises in 7.3 R is assumed to be a ring with 1 (this is crucial for this problem). Also note that IJ is NOT defined to be the set $\{ij : i \in I, j \in J\}$; by definition, IJ is the set of finite sums of elements of the form ij, with $i \in I, j \in J$.
(b) Read the section on the Chinese remainder theorem either in 7.6 or online notes from Lecture 2 (see the Lecture Notes folder in the Resources section on collab).

6. Before formulating this problem, we introduce some notations/definitions.

A. Given a ring R, let $\mathrm{Aut}_{\mathrm{ring}}(R)$ be the set of ring automorphisms of R (that is, bijective ring homomorphisms from R to R). Note that $\mathrm{Aut}_{\mathrm{ring}}(R)$ is a group with respect to composition. Let $\mathrm{Aut}_{\mathrm{group}}(R)$ be the set of group automorphisms of $(R, +)$ (that is, bijections from R to R must preserve addition, but not necessarily multiplication). Again $\mathrm{Aut}_{\mathrm{group}}(R)$ is a group, and it should be clear that $\mathrm{Aut}_{\mathrm{ring}}(R)$ is a subgroup of $\mathrm{Aut}_{\mathrm{group}}(R)$.

B. Given a ring S with 1 and $n \in \mathbb{N}$, define $GL_n(S) = (Mat_n(S))^{\times}$ to be the group of units (=invertible elements) of the ring of $n \times n$ matrices over S. It is not difficult to show that if S is commutative, then a matrix $A \in Mat_n(S)$ lies in $GL_n(S)$ if and only if $\det(A) \in S^{\times}$ (in particular, if S is a field, then $A \in Mat_n(S)$ lies in $GL_n(S)$ if and only if $\det(A) \neq 0$).

Now the actual problem. Let $n \in \mathbb{N}$ and consider $\mathbb{Z}^n$ as a ring with component-wise addition and multiplication (thus $\mathbb{Z}^n$ is just the direct product of n copies of $\mathbb{Z}$). Prove that

(a) $\mathrm{Aut}_{\mathrm{group}}(\mathbb{Z}^n) \cong GL_n(\mathbb{Z})$
(b) $\mathrm{Aut}_{\mathrm{ring}}(\mathbb{Z}^n) \cong S_n$

Hint: In both cases an automorphism is completely determined by where it sends $e_1, \ldots, e_n$, elements of the standard basis of $\mathbb{Z}^n$ (why?) However, there are additional constraints, and these considerably stronger in the case of ring automorphisms.

7.

(a) Let R be a commutative ring with 1, let $X = \{x_1, \ldots, x_n\}$ be a finite subset of R, and let $I = (X)$, the ideal of R generated by X. Prove that (X) is the set of elements of the form $\sum_{i=1}^{n} r_i x_i$ with $r_i \in R$.
(b) State and prove the analogue of (a) without assuming that R is commutative (but still assume that R has 1).
(c) Let F be a field, $n \in \mathbb{N}$ and $R = Mat_n(F)$. Prove that if I is a nonzero ideal of R, then $I = R$.