Algebra II
Fall 2017

Assignment 1.1
Due August 30

Exercise 1. Let $n \in \mathbb{Z}$, $n \neq \square$ (so that $\sqrt{n}$ is irrational;). Show that

$$\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] = \left\{\frac{a+b\sqrt{n}}{2} \;\middle|\; a \equiv b \pmod 2\right\},$$

under the usual arithmetic operations in $\mathbb{C}$, is a ring if and only if $n \equiv 1 \pmod 4$.

Exercise 2. Show that

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b2^{1/3} + c2^{2/3} \mid a, b, c \in \mathbb{Q}\},$$

under the usual arithmetic operations in $\mathbb{C}$, is a ring.

Exercise 3. Let α denote a symbol with the property that $\alpha^2 + \alpha + 1 = 0$. Show that $\alpha \notin \mathbb{Z}_2$ and that

$$\mathbb{Z}_2[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\},$$

under the "natural" arithmetic operations, is a ring. How many elements does it have? Construct a multiplication table for $\mathbb{Z}_2[\alpha]$.

Exercise 4. Let R be a ring, $a, b \in R$ and $m, n \in \mathbb{Z}$. Prove that:

a. $m(ab) = (ma)b = a(mb)$

b. $(ma)(nb) = (mn)(ab)$

Remark. We define $0a = 0$, where the zero on the left belongs to $\mathbb{Z}$ while the zero on the right belongs to R.

Exercise 5. Show that every additive subgroup of $\mathbb{Z}_n$ is a ring.

Exercise 6. Find an integer n that shows the ring $\mathbb{Z}_n$ *need not* have the following "ordinary" properties of $\mathbb{Z}$.

a. If $a \neq 0$, then $ax = b$ has at most one solution.

b. If $a^2 = a$, then $a = 0$ or $a = 1$.

c. If $ab = 0$, then $a = 0$ or $b = 0$.

Exercise 7. Show that if n is prime in the preceding exercise, then statements **a** - **c** are actually valid.

Exercise 8. Let R be a ring and G be an additive abelian group. Given an indeterminate (variable) X consider the formal linear combinations of "powers" of X with exponents coming from G and coefficients in R, i.e. "power series" of the form

$$f = \sum_{g \in G} a_g X^g, \;\; a_g \in R \text{ for all } g \in G. \tag{1}$$

Let $R[[X;G]]$ denote the set of all such objects. Given $f \in R[[X;G]]$ as in (1), the set $\operatorname{Supp} f = \{a_g \neq 0\}$ is called the *support* of f. We now define

$$R[X;G] = \{\, f \in R[[X;G]] \;|\; \operatorname{Supp} f \text{ is finite} \,\},$$

the "polynomials" in R[[X;G]]. We define the sum and product of elements of $R[X;G]$ as follows:

$$\left(\sum_{g \in G} a_g X^g\right) + \left(\sum_{g \in G} b_g X^g\right) = \sum_{g \in G} (a_g + b_g) X^g,$$

$$\left(\sum_{g \in G} a_g X^g\right) \cdot \left(\sum_{g \in G} b_g X^g\right) = \sum_{g \in G} \left(\sum_{h+j=g} a_h b_j\right) X^g.$$

In the final expression the innermost sum runs over all ordered pairs $(h, j) \in G \times G$ so that $h + j = g$.

- **a.** Explain why $R[X;G]$ is closed under the addition and multiplication operations just defined.
- **b.** Prove that $R[X;G]$ is a ring. It is called the *group ring* of G over R.
- **c.** Why might $R[[X;G]]$ with the same operations fail to be a ring? Give an explicit example.
- **d.** What example from class does $\mathbb{Z}[X;\mathbb{Z}]$ reproduce?
- **e.** Describe $\mathbb{Z}[X;\mathbb{Z}_2]$.