Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2017

Thanksgiving Problem Set # 10 (due at the beginning of class on Friday 1 December)

Notation: A **ring homomorphism** between rings S and R is a map $\varphi : S \to R$ preserving the operations $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$. A **ring isomorphism** is a bijective ring homomorphism. The **kernel** of a ring homomorphism is the set of element sent to 0.

Let F be a field. An F**-algebra** A is an F-vector space that is also a ring, with compatibility between multiplication and scalar multiplication $(ax)(by) = (ab)(xy)$ for $a, b \in F$ and $x, y \in A$. An F-algebra A is **unital** if A has 1, and a unital F-algebra homomorphism $\varphi : A \to B$ is required to satisfy $\varphi(1_A) = 1_B$. An F**-subalgebra** of A is an F-subspace that is an algebra under the multiplication in A. To check that a subspace is a subalgebra, it suffices to show that it is closed under multiplication.

Reading: DF 7.2–7.3.

Problems:

1. DF 7.2 Exercises 2, 7, 12 (Hint. Show that $gN = Ng$ for all $g \in G$ thought of as elements in the group ring $R[G]$. Why is this enough?), 13* (Hint: See Exercise 12.).

2. DF 7.3 Exercises 1, 10, 14, 15, 17*, 20, 21* (in particular, if F is a field, find all two-sided ideals of $M_n(F)$), 24, 26*, 28, 29*, 31, 33, 34.

3. *Imaginary quadratic units.* Prove that if $D < 0$, then the group $\mathcal{O}_D^\times$ is finite and find all possibilities for this group. Hint. Think about the topology of the subset $\mathcal{O}_D \subset \mathbb{C}$.

4. *Quaternions.* Let F be a field and $\mathbb{H}_F$ be the ring of F-quaternions, whose elements are

$$a + bx + cy + dz, \qquad a, b, c, d \in F$$

and where addition and multiplication is defined to be the associative and distributive operations with the relations $x^2 = y^2 = z^2 = -1$ and $xy = z = -yx$, $zx = y = -xz$, $yz = x = -zy$. Note that these are the same relations as in the usual (real) quaternions, though the reason why we aren't using i, j, and k will be quickly apparent. As before, $\mathbb{H}_F$ is a unital F-algebra.

(a) Define the 2×2 complex **Pauli matrices**

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These play a role in quantum mechanics. Prove that the $\mathbb{R}$-subspace A of $M_2(\mathbb{C})$ spanned by $I, i\sigma_x, i\sigma_y, i\sigma_z$ is a unital $\mathbb{R}$-algebra isomorphic to $\mathbb{H}_\mathbb{R}$. **Hint.** Realize that $M_2(\mathbb{C})$ is an $\mathbb{R}$-algebra under matrix multiplication, and show that A is an $\mathbb{R}$-subalgebra, so that you only need to check that A is closed under matrix multiplication.

(b) Prove $\mathbb{H}_\mathbb{C}$ is isomorphic, as unital $\mathbb{C}$-algebras, to $M_2(\mathbb{C})$.

(c) For every odd prime p, prove that $\mathbb{H}_{\mathbb{F}_p}$ is isomorphic, as unital $\mathbb{F}_p$-algebras, to $M_2(\mathbb{F}_p)$. **Hint.** The idea is to find replacements for the Pauli matrices. First, if -1 is a square in $\mathbb{F}_p^\times$, then you can literally use the Pauli matrices, replacing i by a square root of -1. Prove that for p odd, -1 is a square in $\mathbb{F}_p^\times$ if and only if $p \equiv 1 \pmod 4$. To do this, recall the (as of yet unproved) fact that $\mathbb{F}_p^\times$ is a cyclic group of order $p - 1$, which is even since p is odd. Then the squares will form a subgroup of index 2 in $\mathbb{F}_p^\times$ and in fact any element of order 4 in $\mathbb{F}_p^\times$ will be a square root of -1. But $\mathbb{F}_p^\times$ has an element of order 4 if and only if $p - 1$ is divisible by 4. So what about the case $p \equiv 3 \pmod 4$? Here, you need to come up with different matrices whose square is $-I$, which by linear algebra, must have trace 0 and determinant 1. The following fact will be useful: when p is odd, there are $(p + 1)/2$ squares in $\mathbb{F}_p$ (this following immediately from the preceding discussion, together with the fact that 0 is a square).

(d) Prove that $\mathbb{H}_{\mathbb{F}_2}$ is isomorphic to the group ring $\mathbb{F}_2[G]$, where G is a Klein-four group.