Yale University Department of Mathematics
Math 350 Introduction to Abstract Algebra
Fall 2016

Problem Set # 9 (due at the beginning of class on Friday 18 November)

Notation: Let R and S be rings. A **ring homomorphism** between S and R is a map $\varphi : S \to R$ that is a homomorphism of the underlying abelian groups and is multiplicative, i.e., $\varphi(x+y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$. A **ring isomorphism** is a bijective ring homomorphism.

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

Reading: DF 7.1–7.3.

Problems:

1. DF 7.1 Exercises 3, 4, 6, 7, 13, 14* (Hint. $(1+x)(1-x) = 1 - x^2$ will help you if $x^2 = 0$, what do you do if $x^n = 0$?), 15, 21* (Venn diagrams are ok!), 29, 30* (cf. notations in 28).

2. DF 7.2 Exercises 2, 3*, 7, 12* (Hint. Compute $e_g N$ for all $g \in G$, where e_g are the generators of the group ring $R[G]$), 13.

3. *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 that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, which is even since p is odd. By the classification of subgroups of a cyclic group, 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.