MA 294: Applied Abstract Algebra / Spring 2022
Homework assignment #10
Due Thursday 4/21/2022 by 4pm
Ok to turn in late, but don't wait to work out the problems!

Turn in your work either in class or before 4pm in the envelope hanging on MCS 127.

- Please staple or otherwise connect the pages of your work. There is a stapler in the math department main office. Yes, this requires a tiny bit of planning — but I know we can do this! Our grader is anxious that homework set pages might get lost.
- Write your name on the front page. Plan ahead: perhaps you need to carry around a pen for this purpose on Thursdays?
- Consider using a pen rather than a pencil, especially if your pencilwork is smudgy.

Read sections 22.1, 22.2, 22.3, 22.4.

(1) Exercise 22.9.9

(2) Exercise 22.1.3

(3) Exercise 22.2.3

(4) Exercise 22.4.1

(5) In class, we showed that if R is a commutative ring, then $M_2(R)$ is also a ring under matrix addition and matrix multiplication.

  (a) How many elements are there in $M_2(\mathbb{Z}_2)$?

  (b) Which elements of $M_2(\mathbb{Z}_2)$ are invertible? How many are there?

  (c) By Theorem 22.2 the set of invertible elements of $M_2(\mathbb{Z}_2)$ is a group. Which of the groups that we have studied is this group isomorphic to?

(6) For $f(x), g(x)$ in $\mathbb{Z}_2[x]$, say that $f(x) \equiv_{x^2+x+1} g(x)$ if there exists a polynomial $h(x) \in \mathbb{Z}_2[x]$ so that $f(x) - g(x) = h(x)(x^2 + x + 1)$. In other words, $f(x) \equiv_{x^2+x+1} g(x)$ if their difference is a polynomial that is divisible by $x^2 + x + 1$. Convince yourself that "congruence modulo $x^2 + x + 1$" is an equivalence relation on $\mathbb{Z}_2[x]$ — the argument is very similar to showing that "congruence modulo m" is an equivalence relation on $\mathbb{Z}$, and you do not need to write this up.

  Write $\mathbb{Z}_2[x]_{x^2+x+1}$ for the set of equivalence classes of $\mathbb{Z}_2[x]$ under the relation $\equiv_{x^2+x+1}$. Convince yourself that addition and multiplication is well-defined for elements of $\mathbb{Z}_2[x]_{x^2+x+1}$ — again, the argument is completely analogous to the well-definition of addition and multiplication on $\mathbb{Z}_m$, and again, you do not need to write this up.

  It follows that $\mathbb{Z}_2[x]_{x^2+x+1}$ is a commutative ring.

  (a) How many elements are in $\mathbb{Z}_2[x]_{x^2+x+1}$? Find representatives for each equivalence class.

  (b) Make an addition table for $\mathbb{Z}_2[x]_{x^2+x+1}$.

  (c) Make a multiplication table for $\mathbb{Z}_2[x]_{x^2+x+1}$.

  (d) Show that $\mathbb{Z}_2[x]_{x^2+x+1}$ is a field.