MATH 123 - ALGEBRA II - SPRING 2020
ASSIGNMENT 4

Due Tuesday, February 25, 11h59pm. (please submit your assignment as a PDF on Canvas). Unless otherwise noted, references are to Dummit and Foote, *Algebra*, 3rd edition, Wiley, 2004.

Remember that in this class "ring" means "ring with identity".

Practice problems

(*Not* for credit. No need to submit your solutions. Try to do them while minimally looking at the textbook)

(1) Give the definition of the following: degree, monic, module, submodule, module homomorphism, free module of rank n, direct product of modules, cyclic module.
(2) State and prove Gauss' lemma.
(3) State and prove Eisenstein's criterion.
(4) State and prove the relationship between irreducibility of a polynomial and having a root.
(5) Explain why $\mathbb{Z}$-modules are the same as abelian groups, and why an $F[x]$-module (F a field) is the same as a vector space V over F plus a linear transformation from V to itself.
(6) True or false?
   (a) If R is a UFD with field of fractions F, then a polynomial in $R[x]$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$.
   (b) If F is a field and a polynomial $f(x)$ does not have a root in F, then it is irreducible.
   (c) A degree one polynomial is always irreducible.
   (d) If R is a commutative ring, then it is naturally an R-module and its R-submodules are exactly its ideals.
   (e) If $V = \mathbb{R}^2$ (as an $\mathbb{R}$-vector space), and $T : \mathbb{R}^2 \to \mathbb{R}^2$ is the linear transformation given by 90 degrees counterclockwise rotation, then the $\mathbb{R}[x]$-module induced by (V, T) is cyclic.
   (f) If M is an R-module and $m \in M$ is not zero, then $m + m$ is not zero.

Problems for credit

(1) You should have the assignment from another student available for review in your Canvas todo list. Review problem 7 from that assignment (submit your comment on Canvas, *not* with this assignment). Refer to the peer review instructions on the course website for more details. *You are encouraged not to look at the official solution before submitting your review!*
(2) Let R be an integral domain. A polynomial in $R[x]$ is called a *monomial* if it is of the form ax^k for $a \in R$ and $k \geq 0$. Prove that if $f(x), g(x) \in R[x]$ are not zero, then $f(x) \cdot g(x)$ is a monomial if and only if both f and g are monomials. *[Remark: this explains in particular why both constant coefficients are zero in the proof of Eisenstein's criterion.]*
(3) (a) (DF, 9.2.2) Let F be a field with q elements and let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements.
   (b) (DF, 9.2.3) Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Prove that $F[x]/(f(x))$ is a field if and only if f is irreducible.
   (c) (DF, 9.4.6) Construct fields with the following number of elements: 9, 49, 8, and 81.

Date: February 24, 2020.

(4) (DF, 9.3.4) Let R be the set of polynomials in $\mathbb{Q}[x]$ whose constant term is an integer (you should convince yourself that this is a subring of $\mathbb{Q}[x]$).
  (a) Prove that R is an integral domain with units ± 1.
  (b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$, and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant term ± 1. Prove that all these irreducibles are prime in R.
  (c) Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible). Conclude that R is not a UFD.
  (d) Show that (x) is not prime in R and describe units and zero divisors in the quotient ring $R/(x)$.

  [Remark: DF, 9.3.5 establishes that R is in fact a Bezout domain.]

(5) (DF, 9.4.1) Determine whether the following polynomials are irreducible in the ring indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes $\mathbb{Z}/p\mathbb{Z}$ for p a prime.
  (a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$.
  (b) $x^3 + x + 1$ in $\mathbb{F}_3[x]$.
  (c) $x^4 + 1$ in $\mathbb{F}_5[x]$.
  (d) $x^4 + 10x^2 + 1$ in $\mathbb{Z}[x]$.

(6) (DF, 9.4.18) Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$. Are they also irreducible in $\mathbb{Z}[x]$? *[Hint: generalize Eisenstein's criterion to non-monic polynomials].*

(7) Recall there is a correspondence between $\mathbb{Z}$-modules and abelian groups. What object(s) correspond to $\mathbb{Z}[x]$-modules?

(8) (DF, 10.1.8) An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero $r \in R$. The set of torsion elements of M is denoted $\mathrm{Tor}(M)$.
  (a) Prove that if R is an integral domain, then $\mathrm{Tor}(M)$ is a submodule of M (called the *torsion submodule of* M.)
  (b) Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule of M *[Hint: consider R itself].*
  (c) If R has nonzero zero divisors, show that every nonzero R-module has nonzero torsion elements.