Math 500: HW 8 due Friday, October 20, 2023.

1. Let K be a finite field of order q. Show that in $R = K[x]$ there are exactly (i) q monic irreducible polynomials of degree 1 and (ii) $(q^2 - q)/2$ monic irreducible polynomials of degree 2. (Hint: there are exactly q^k monic polynomials of degree k, so instead count the reducible ones.)

2. Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2 + 1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2 + 2y + 2)$ are both fields with $11^2 = 121$ elements. Prove that the map which sends the element $p(\overline{x})$ of K_1 to the element $p(\overline{y} + 1)$ of K_2 is well-defined and gives a ring isomorphism from K_1 to K_2.

3. Let F be a field. Prove that $F[x]$ contains infinitely many prime elements. Hint: modify Euclid's proof of the infinitude of primes in $\mathbb{Z}$.

4. Prove that $x^2 + y^2 - 1$ is irreducible in $\mathbb{Q}[x, y]$.

5. This exercise produces a non-Noetherian ring (in fact, as a subring a Noetherian ring). Let F be a field, and consider the polynomial ring $R := F[x, y] = F[x][y]$. Any $f(x, y) \in R$ can be written $f_0(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_n(x)y^n$ where $n \geq 0$ and all $f_k(x) \in F[x]$.

    (a) Consider $S = \{a + y \cdot g(x, y) \mid a \in F \text{ and } g(x, y) \in R\} \subseteq R$; equivalently, S consists of $f \in R$ where the $f_0(x)$ above is in F. Show that S is a subring (with 1) of R.

    (b) Let $I_k \subseteq S$ be the ideal of S generated by the subset $\{y, xy, \ldots, x^{k-1}y\}$. Show that if $f(x, y) = \sum f_i(x)y^i$ is an element of I_k, then $\deg_x f_1(x) < k$ (meaning degree as a polynomial in x).

    (c) Conclude that for all k we have that $x^k y \notin I_k$. Use this to show that S is not Noetherian.

6. Let R be a commutative ring, and let M be a module with submodules $N_1, N_2 \subseteq M$. Show that if $N_1 \cap N_2 = 0$ and $N_1 + N_2 = M$, then there are R-module isomorphisms $M/N_1 \approx N_2$ and $M/N_2 \approx N_1$.

7. Let R be a commutative ring with 1. Given an ideal I of R and an R-module M, define:

$$IM = \left\{ \sum_{\text{finite}} a_i m_i \;\middle|\; a_i \in I,\ m_i \in M \right\}.$$

    (a) Prove that IM is a submodule of M.

    (b) Show that if $IM = 0$, then M can be given the structure of an R/I module, with action defined by $\overline{r} \cdot m := r \cdot m$.

8. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \approx \mathbb{Z}/d\mathbb{Z}$, where $d = \gcd(m, n)$.

9. Let N be a submodule of M. Prove that if both M/N and N are finitely generated then so is M.

Credit: Problems 1, 5, 6, and 7(b) are from [R] and the rest from [DF].