Lecture 23: Polynomial miscellanea; Noetherian rings; Modules 101.

§41-46 of [R2].
§9.4, 9.5 and 10.1 of [DF].

Previously, **Thm** $R[x]$ a UFD $\Leftrightarrow$ R is a UFD.

Prop: R a comm. ring with 1, $I \subsetneq R$ an ideal. Suppose $p \in R[x]$ is monic and nonconst. If $\overline{p}(x)$ is irred in $(R/I)[x]$ then $p(x)$ is irred in $R[x]$.

Eisenstein criterion: $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ a monic poly in $\mathbb{Z}[x]$. If there is a prime p with $p \mid a_i$ for all i but $p^2 \nmid a_0$ then $f(x)$ is irreducible.

Ex: $f(x) = x^n - 2$ is irred in $\mathbb{Q}[x]$. By Gauss, equiv to $x^2 - 2$ is irred in $\mathbb{Z}[x]$. Now use Eisenstein with $p = 2$.

Pf: If $f(x) = a(x)\,b(x)$, then $x^n = \overline{a}(x) \cdot \overline{b}(x)$ in $(\mathbb{Z}/(p))[x]$. So const. terms of $\overline{a}, \overline{b}$ are 0. Hence $p \mid$ const terms of $a, b \Rightarrow p^2 \mid a_0$, a contradiction. ▨

[Note also have Eisenstein for other int. domains, replace p with a prime ideal $P \subseteq R$.]

Prop: R int domain. Then $f \in R[x]$ has at most $\deg f$ roots in R.

Pf: Set $F = \mathrm{Frac}(R)$. If $a \in F$ is a root of f, saw last time that $f(x) = (x-a)\cdot q(x)$. If $f(b) = 0$ with $a \neq b$, get $q(b) = 0 \Rightarrow q(x) = (x-b)\,g(x)$. The claim now follows as $F[x]$ is a UFD. ▨

[Skip the rest of the page, come back to if time at end.]

Thm: F a field, G a finite subgp of $F^\times$. Then G is cyclic.

Pf: Have $G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$ where each $n_i \mid n_{i+1}$. If $k \geq 2$, have at least n_1^2 elts with $g^{n_1} = 1$, namely $\langle a_1, a_2^{n_2/n_1} \rangle \cong C_{n_1} \times C_{n_1}$. But then $X^{n_1} - 1$ has more than n_1 roots, contradicting the proposition. ▨

($C_{n_1} = \langle a_1 \rangle$, $C_{n_2} = \langle a_2 \rangle$)

A comm ring with 1 is *Noetherian* if every ideal is finitely generated.

Ex: PIDs, e.g. $\mathbb{Z}$, any field.

Thm: A comm ring R with 1 is *Noetherian* $\Leftrightarrow$ it has the ascending chain condition for ideals.

Pf: §43 of [RZ]. [Same idea as for acc for subgroups $\Leftrightarrow$ all subgps are finitely generated.]

Hilbert Basis Thm: If R is *Noetherian*, so is $R[x]$.

Cor: For any field, $\mathbb{F}[x_1, x_2, \dots, x_n]$ is *Noetherian*.

[See §43 of [RZ] for a proof. Very useful in alg. geom.]

R a ring with 1. A *(left) R-module* is an abelian group $(M, +)$ with a fn $R \times M \longrightarrow M$, $(r, m) \longmapsto r \cdot m$ satisfying:

a) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$

b) $1 \cdot m = m$.

c) $(r_1 + r_2) \cdot m = r_1 m + r_2 m$

d) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

Ex: If R is a field, an R-module is exactly an R-vector space.

Ex: Any abelian group $(M,+)$ is a $\mathbb{Z}$-module; For $a \in \mathbb{Z}_{\geq 0}$, set $a \cdot m = \underbrace{m+m+\cdots+m}_{a \text{ times}}$ and $(-a)\cdot m = -(a\cdot m)$.

Note: For any R-module M, $0 \cdot m = 0$ for all m as $0m = (0+0)\cdot m = 0m + 0m$. (0 ← zero in R) Also $(-1)\cdot m = -m$ as $0 = 0\cdot m = (1+(-1))\cdot m = 1\cdot m + (-1)\cdot m$.

Ex: R any ring. The free module of rank n is $R^n = \{(a_1, \ldots, a_n) \mid a_i \in R\}$ with componentwise addition and module str $r\cdot(a_1, a_2, \ldots, a_n) := (ra_1, ra_2, \ldots, ra_n)$.

A submodule of an R-module M is a subset $N \subseteq M$ such that ① $(N,+)$ is a subgp of $(M,+)$ and ② for all $r \in R$ and $n \in N$ we have $r \cdot n \in N$.

Ex: For R a field a submodule is a subspace.

Ex: For $R = \mathbb{Z}$ a submodule is just a subgp.

Ex: R comm, $M = R^1$. A submod of M is an ideal.

A homomorphism $\psi: A \to B$ of R-modules is a hom of $(A,+) \to (B,+)$ where

$$\psi(r \cdot a) = r \cdot \psi(a) \text{ for all } r \in R \text{ and } a \in A.$$

Ex: For R a field, these are linear transformations.