NAP 2018, NOTES ON CLASS #5, 15 MAY, 2018

• We extended Corollary 1.9.3 (to Euclid's Lemma 1.9.2) to
Corollary 1.9.3′: Let R be a PID, $s \in \mathbb{N}$ and $p, a_1, a_2, \ldots, a_s \in R$. If p is irreducible and $p \mid a_1 \cdot a_2 \cdot \ldots \cdot a_s$, then $p \mid a_i$, for some i.

• We used this for the proof of
Theorem 1.9.4: If F is a field then $F[X]$ is a UFD.
Actually the two parts we did show that

1. If R is a Euclidean domain (Euclidean means "has a degree and division algorithm", such as $\mathbb{Z}$ and $F[X]$), then every non-zero non-unit of R is a finite product of irreducible elements of R, and
2. If R is a PID, then such a factorization is unique in the sense that, if $p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$, and the p_i, q_j are irreducible, then $n = m$ and there exists a re-ordering of $\{q_1, q_2, \ldots, q_n\}$ so that each $p_i = u_i q_i$ for some unit u_i.

True Theorem: Every PID is a UFD (won't prove).

• Didn't prove, PLEASE READ, related to item 1.7 p. 9:
Proposition 1.7.0: Let F be a field and $f(X) \in F[X]$. Then
$$\#\{\text{distinct roots of } f(X) \text{ in } F\} \leq \deg f(X).$$

• **Proposition 1.18.** Irreducibility mod p test for $\mathbb{Z}[X]$. Let $f(X) \in \mathbb{Z}[X]$:

1. If $f(X) = g(X)h(X)$, where $g(X), h(X) \in \mathbb{Z}[X]$, then the images in $\mathbb{F}_p[X]$ satisfy $\overline{f(X)} = \overline{g(X)} \cdot \overline{h(X)}$, for every prime element p of $\mathbb{Z}$.
2. If $f(X)$ factors nontrivially in $\mathbb{Z}[X]$, then $\overline{f(X)}$ factors nontrivially in $\mathbb{F}_p$, for every p with $\deg f(X) = \deg \overline{f(X)}$, i.e. for every p that does NOT divide the leading coefficient of $f(X)$.
3. If $f(X)$ is primitive and there exists a prime element $p \in \mathbb{Z}$ such that p does NOT divide the leading coefficient of $f(X)$ and $\overline{f(X)}$ is irreducible mod p, then $f(X)$ is irreducible in $\mathbb{Z}[X]$, hence also in Q$[x]$, by Gauss' Lemma 1.13.

• Began field extensions [p. 13 of book]. Defined E/F, the field extension E over F, for $F \subseteq E$, fields. Discussed $F[\alpha]$, the smallest *subring* of E containing F and α [p.14], and $F(\alpha)$, the smallest *subfield* of E containing F and α [p. 15], for E, F fields and $\alpha \in E$. Considered examples $\mathbb{Q}[\sqrt{2}], \mathbb{Q}(\sqrt{2}), \mathbb{Q}[i], \mathbb{Q}(i), \mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Showed $\mathbb{Q}[i] = \mathbb{Q}(i)$, $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

• Defined *degree* of the extension E/F, for $F \subseteq E$, fields, to be the vector space dimension of E as an F-vector space. Began discussion for
Proposition 1.20 [p. 14]: If $F \subseteq E \subseteq L$ are fields, and the degrees of L/E and E/F are both finite, then the degree of L/F is finite and is equal to the product of the degrees of L/E and E/F. Conversely, if the degree of L/F is finite, then the degrees of L/E and E/F are both finite.