NAP 2018, NOTES ON CLASS #4, 14 MAY, 2018

• We proved the book's version [1.13] of Gauss's Lemma, again carefully explaining what "non-trivially means". We emphasized that the book's version is really the main point, and that the version proved in Class 3, that the product of primitive polynomials is primitive, is just a tool. The key to deducing 1.13 from the version done in Class 3 is the following observation: If $f(X)$ is a primitive polynomial in $\mathbb{Z}[X]$ and c is a non-zero rational number such that $cf(X)$ is also a primitive polynomial in $\mathbb{Z}[X]$, then $c = \pm 1$.

• Professor Ajaya Singh came by to take a class photo. (Actually, about $2^{\aleph_1}$ photos were taken, by the time everyone's cellphone had been satisfied.)

• [Remarks 1.4] Reminder of Freshman's Dream in characteristic $p > 0$, and Frobenius homomorphism.

• [Remarks 1.5] Quick review of vector spaces, linear independence, spanning, bases, dimension. If F is a field, $F[X]$ is a vector space over F. Pointed out that $\{1, X, X^2, \dots\}$ is a basis for $F[X]$, so $F[X]$ is an infinite-dimensional vector space over F.

• Reminder of formal definition of GCD. We proved the long-awaited Theorem 1.8: If R is a PID, (1) a GCD of two non-zero elements exists and (2) the GCD can be expressed as a linear combination of the two elements. We reminded that (3) If R is Euclidean (has a degree and division algorithm. e.g., in $\mathbb{Z}$ or $F[X]$ where F is a field), then repeated use of the algorithm yields the GCD and the coefficients of such a linear combination. Students were directed to the book [1.8, p. 10] for the details and encouraged to work examples (one of which occurs on Homework #2).

• [Material related to 1.6 and 1.9 in book:] Reminder [1.9.1] $F[X]$ is a PID. Reminder of result from Class #3, Euclid's Lemma 1.9.2: In a PID, if $a \mid bc$ and $\mathrm{GCD}(a, b) = 1$, then $a \mid b$. Special case, Corollary 1.9.3: If p is irreducible and $p \mid ab$, then $p \mid a$ or $p \mid b$. Note $\mathrm{GCD}(a, b)$ is defined only up to units. In other words, if d is a GCD of a and b, and $e \in R$, then e is a GCD of a and b if and only if there is a unit u of R such that $e = du$. Thus "$\mathrm{GCD}(a, b) = 1$ just means that units are the only common divisors of a and b.

• [Related to 1.6 and 1.9 in book:] Definition of UFD; began proof of Theorem 1.9.4: If R is Euclidean (has a degree and division algorithm), then R is a UFD (unique factorization domain) but ran out of time. We did manage to show that every non-zero non-unit is a product of irreducibles. Proof of uniqueness is first on the agenda for Class #5. Actually every PID is a UFD (won't prove).

• We found, to our dismay, that students cannot access the notes and other handouts, which have been faithfully posted, by Nilu, on the NAP website. This resulted in a late-night email frenzy. (Apparently students can send and receive emails but cannot access the internet. Strange!)