NAP 2018, NOTES ON CLASS #3, 10 MAY, 2018

• In a PID, if $a \mid bc$ and a and b are relatively prime (have GCD = 1), then $a \mid c$ (Sometimes called "Euclid's Lemma, related to [Book 1.9].) (We proved this assuming the Euclidean Algorithm, that is, the GCD of two things is a linear combination of the two things, related to [Book 1.8].) We also used:

• The "Two-out-of-Three" Lemma: In a commutative ring, if $a \pm b = c$ and two of a, b, c are divisible by some element r, then so is the third. Related to [Book 1.9].) (We proved one of the six cases, leaving the rest to the students' imagination and amusement.)

• "Impossible Rational Roots Theorem" (Proposition 1.11 in book): Let $f(X) \in \mathbb{Z}[X]$ and let $r \in \mathbb{Q}$ be a root of $f(X)$. If $r = \frac{m}{n}$ in "lowest terms" (that is, m and n are relatively prime integers), then m divides the constant term of $f(X)$ and n divides the leading coefficient. This cuts the search for roots down to a finite problem. In particular, if $f(X)$ is monic, to test for rational roots you need only try (positive and negative) divisors of the constant term. This is particularly useful for determining whether or not a cubic polynomial is irreducible in $\mathbb{Q}[X]$. (Some people call this the "Possible Rational Roots Theorem". Question: Is 1 a "possible rational root" of $X^2 + 1$?)

• We gave a detailed proof of the "Impossible Rational Roots Theorem" and discussed Eisenstein's Criterion [Book 1.16]), without giving the proof. Warning: Many polynomials are not Eisensteinable. If there is no prime satisfying the requirements of Eisenstein's Criterion, the test is inconconclusive: the polynomial may or may not be irreducible; use another approach. (For example, consider $X^2 + 1$ and $X^2 - 1$.)

• In trying to determine whether or not a polynomial $f(X) \in \mathbb{Q}[X]$ is irreducible, we quickly reduce to the case of polynomials in $\mathbb{Z}[X]$ by clearing denominators. Recall that a polynomial in $\mathbb{Q}[X]$ is irreducible if and only if it is non-constant and cannot be factored as a product of two non-constant polynomials. Thus, for a non-zero $c \in \mathbb{Q}$, we see that $f(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if $cf(X)$ is irreducible. Taking c to be the product (or maybe the least common multiple) of the denominators of $f(X)$, we obtain a polynomial in $\mathbb{Z}[X]$.

• We defined "primitive polynomial" (an integer polynomial for which the GCD of the coefficients is 1) and proved *our* version of Gauss's Lemma [Book 1.13]: The product of two primitive polynomials is primitive. (Sketch: $f(X) \in \mathbb{Z}[X]$ is primitive if and only if its reduction modulo p is non-zero in $\mathbf{F}_p$ for every prime p. Now GL follows from the fact that $\mathbf{F}_p[X]$ is a domain for each p, and the fact that reduction mod p is a homomorphism, that is, $\overline{gh} = \overline{g}\overline{h}$. We did not have time to prove the book's version of GL but will do so next week. By the way, one must interpret "factors non-trivially" in the book's version to mean "factors as a product of two non-constant polynomials". Note, for example, that $2X^2 + 2$ is irreducible in $\mathbb{Q}[X]$ but not in $\mathbb{Z}[X]$. Precise definitions are important (at least to pedants like us).

• We gave examples from time to time to illustrate stuff and had a brief discussion of the binomial theorem, Freshman's Dream and characteristic p [Book 1.4].