Math 418H **Fall 2005**

Lecture: Wed 9/28/05

1. Why define abstract structures like a field or a Euclidean ring, rather than just prove things for $\mathbb{Q}$ and $\mathbb{Z}$ directly?

   - The field axioms are the crucial properties of $\mathbb{Q}$, which give a foundation from which to rigorously prove most of the formulas of algebra. Similarly, the crucial properties of $\mathbb{Z}$ are captured in the definition of a Euclidean ring, giving us a foundation to prove non-obvious facts such as Unique Factorization.
   - Once we prove a formula using only the field axioms, we know it holds not only for $F = \mathbb{Q}$, but for *any* new field we may define, such as the clock arithmetic field $\mathbb{Z}_p$ (p prime) or the rational functions $\mathbb{Q}(x)$. Similarly,since Unique Factorization depends only on the division algorithm, we know it holds not only for $\mathbb{Z}$ but for $\mathbb{Q}[x]$ and any other Euclidean ring we find.

2. Basic formulas for any field F

   - We assume axioms (i)–(iv), (i')–(iv'), (v). In the proofs, we will use commutativity and associativity without comment.
   - *Lemma:* The elements 0, 1, $-a$, a^{-1} are unique.
     Proof: If we have two zero elements $0, 0'$ with $a + 0 = a + 0' = a$ for all a, then: $0 = 0 + 0' = 0'$. If we have two inverse elements $-a, -a'$ with $(-a) + a = (-a') + a = 0$, then:

     $$\begin{aligned} -a &= (-a) + 0 \\ &= (-a) + a + (-a') \\ &= 0 + (-a') = -a'\,. \end{aligned}$$

     Similarly for 1 and a^{-1}.
   - *Lemma:* $0 \bullet a = 0$
     Proof:
     $$\begin{aligned} 0 &= -(0 \bullet a) + 0 \bullet a \\ &= -(0 \bullet a) + (0{+}0) \bullet a \\ &= -(0 \bullet a) + 0 \bullet a + 0 \bullet a \\ &= 0 \bullet a\,. \end{aligned}$$
   - *Lemma:* $-(-a) = a$
     Proof:
     $$\begin{aligned} -(-a) &= -(-a) + 0 \\ &= -(-a) + (-a) + a \\ &= 0 + a = a\,. \end{aligned}$$

- *Lemma:* $(-a) \bullet b = -(a \bullet b)$
  Proof: By definition, $-(a \bullet b)$ is the unique element such that $-(a \bullet b) + a \bullet b = 0$. Now:
  $$\begin{aligned}(-a) \bullet b + a \bullet b &= ((-a) + a) \bullet b \\ &= 0 \bullet b \;=\; 0\,.\end{aligned}$$
- *Lemma:* $(-a) \bullet (-b) = a \bullet b$
  Proof: Using the previous lemma twice:
  $$\begin{aligned}(-a) \bullet (-b) &= -(a \bullet (-b)) \\ &= -(-(a \bullet b)) = a \bullet b\,.\end{aligned}$$

3. Advanced formulas for any field F

- Prove the following as exercises.
- Quadratic formula: The only roots of $ax^2 + bx + c \in F[x]$ are $x = (-b \pm d)/2a$, where $d \in F$ is an element with $d^2 = b^2 - 4ac$. If there is no such element $d \in F$, then the equation has no solution.
- FOIL: $(a+b)(c+d) = ac + ad + bc + bd\,.$
  This holds in any commutative ring, not necessarily a field.
- Binomial Theorem:
  $$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2 \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3 \\ (a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\ (a+b)^n &= a^n + \tbinom{n}{1}a^{n-1}b + \tbinom{n}{2}a^{n-2}b^2 + \cdots + b^n\,,\end{aligned}$$
  where the binomial coefficients $\binom{n}{k}$ are defined recursively by:
  $$\tbinom{n}{0} = \tbinom{n}{n} = 1 \qquad \text{and} \qquad \tbinom{n+1}{k} = \tbinom{n}{k} + \tbinom{n}{k-1}\,.$$
  Again, this holds in any commutative ring.
- *Example:* In $F = \mathbb{Z}_2$, we have $2 = 0$, so $(a+b)^2 = a^2 + b^2$. This is not so remarkable, since $\mathbb{Z}_2$ has only two elements. But now consider $\mathbb{Z}_2[x]$, polynomials with coefficients in $\mathbb{Z}_2$. For example:
  $$f(x) = 0\,,\ 1\,,\ x\,,\ x{+}1\,,\ x^2\,,\ x^2{+}1\,,\ x^2{+}x\,,\ x^2{+}x{+}1\,,\ \ldots$$
  Then we once again have:
  $$(f(x) + g(x))^2 = f(x)^2 + g(x)^2$$
  for any polynomials $f(x), g(x) \in \mathbb{Z}_2[x]$.
- $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots ab^{n-2} + b^{n-1})$.