L13 (April 6, 2020) I will start this lecture with a nice exercise/problem for you. In fact, with two of them. But first I have to ~~define~~ introduce an important class of rings. We say that a ring R is an integral domain if for every $a, b \in R$ we have: $ab = 0_R \Rightarrow a = 0_R$ or $b = 0_R$. For example, $\mathbb{Z}$ is an i.d. but $\mathbb{Z}_6$ is not because $\bar{2} \cdot \bar{3} = \bar{0}$ in $\mathbb{Z}_6$.

Proposition If R is a finite integral domain then R is a field (every $a \in R$, $a \neq 0_R$, has a multiplicative inverse). Proof is **Problem 13.1.** Prove this proposition. Hint: for any $a \in R$, $a \neq 0_R$, consider the map $x \mapsto ax$ from $R \setminus \{0_R\}$ to itself. From this we get another **Proposition** If $m \in \mathbb{N} \setminus \{1\}$ then the ring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ (of residue classes modulo m) is a field $\Leftrightarrow m = p$, i.e. m is a prime number.

Proof. **Problem 13.2.** Prove this proposition. Hint: use the previous proposition. An interesting result related to the last but one proposition but which is

much deeper and harder to prove is the following.

Theorem (J. Wedderburn, 1905) There is no finite skew field (a field with non-commutative multiplication). That is, every non-commutative field has to be infinite. For a proof see the book M. Aigner & G. Ziegler: Proofs from THE BOOK. A point of interest is that a "group-theoretic" proof was published in a 2 page note in 1964 by Theodore Kaczynski who later became the Unabomber, see Wikipedia for the whole story. An example of a non-comm. field is the field of quaternions $\mathbb{K} = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{R}\}$ where $i^2 = j^2 = k^2 = -1$ and $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$ and $ik = -j$ and otherwise we add and multiply in $\mathbb{K}$ in the "obvious" way. For example,

$(2+3i-4j+k) + (-1-i+j-2k) = 1+2i-3j-k$,

$(2+3i-4j+k)\cdot(-1-i+j-2k) = (-2-2i+2j-4k) + (-3i+3+3k+6j) + (4j-4k+4+8i) + (-k-j-i+2) =$

$= 7+2i+11j-6k$. Since the multiplication is

non-commutative, in the other order we get:
$(-1-i+j-2k)\cdot(2+3i-4j+k) = (-2-3i+4j-k)+$
$+(-2i+3+4k+j)+(2j-3k+4+i)+(-4k-6j-8i+2) =$
$= 7-12i+j-4k.$

So every commutative finite field is! but how do the fin. fields look like? We eventually prove: $\forall n\in\mathbb{N}$ $\forall$ prime number p $\exists$ field $F: |F| = p^n$. I leave the opposite implication (if F is a fin. field then $|F| = p^n$) for you as an exercise but first, to make the proof easier for you, I recall further notions from comm. algebra.

Proposition/Definition If R is an integral domain and $n\in\mathbb{N}$ for $n_R := \underbrace{1_R+1_R+\dots+1_R}_{n\ 1_R's}$ then either
*) denoted $\mathrm{char}(R)$
$n_R \neq 0_R$ for every $n\in\mathbb{N}$ or the minimum $n\in\mathbb{N}$ s.t. $n_R = 0_R$ is a prime number, $n=p$. In the former case we say that R has characteristic 0*) and in the latter case that R has characteristic p. **Proof.**

If $n_R = 0_R$ and $n = k\ell$, $k,\ell\in\mathbb{N}$, then
$k_R \cdot \ell_R = \underbrace{(1_R+1_R+\dots+1_R)}_{k}\cdot\underbrace{(1_R+1_R+\dots+1_R)}_{\ell} =$

$= 1_R 1_R + \cdots + 1_R 1_R = \underbrace{1_R + \cdots + 1_R}_{n} = n_R = 0_R$. Since R is an integral domain, $n = rs$, $r_R = 0_R$ or $s_R = 0_R$. If n is minimum with $n_R = 0_R$ then $n = rs$ implies that $r = n$ or $s = n$ and n is a prime number. ☒

If F is any field, finite or infinite, the prime field GC F is the subfield of F generated by applying $+$ and $\cdot$ and: to the elements 0_F and 1_F. More briefly, it is the smallest (to $\subset$) subfield of F.

For example the prime field of the fields $\mathbb{R}$ and $\mathbb{C}$ (the real and complex numbers) is the field $\mathbb{Q}$ (the rational numbers). More generally, the prime field of any field F with $\mathrm{char}(F) = 0$ is $\mathbb{Q}$. It is easy to see that the prime field of any field F with $\mathrm{char}(F) = p$ is the field $\mathbb{Z}_p$ (see Problem 13-2).

Proposition If F is a finite field then there exist a $n \in \mathbb{N}$ and a prime number p s.t. $|F| = p^n$.

Proof. **Problem 13-3.** Prove this proposition. Hint: Such F forms also a vector space over its prime field $\mathbb{Z}_p$.

To go in the other way and to actually construct for each q and p a field with p^2 elements, we still have to recall ideals in rings. **Definition** If R is a ring and $I \subset R$, $I \neq \emptyset$, we say that I is an ideal (in R) if: • $a, b \in I \Rightarrow a - b \in I$,

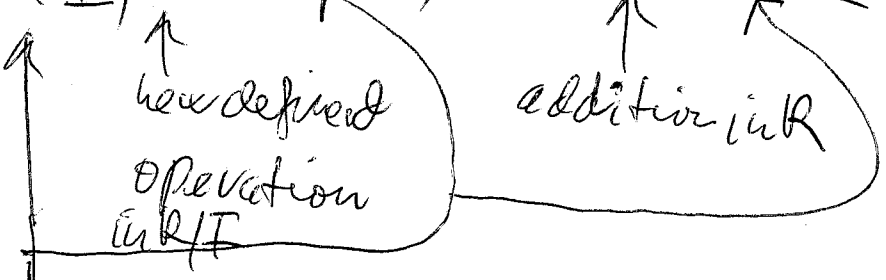
• $a \in I, b \in R \Rightarrow ab \in I$. In other words, an ideal in R is an Abelian subgroup of the Abelian group $(R, 0_R, +)$ that is closed under multiplication by any element from R. Two kinds of ideals are very important: $I \subset R$ is a maximal ideal if $I \neq \{0_R\}$ ($\{0_R\}$ is an ideal, the zero ideal), $I \neq R$ and if $J \subset R$ is an ideal with $J \supsetneq I$ then $J = R$ (R is another trivial ideal in R). $I \subset R$ is a prime ideal in R if it has the property that: $a, b \in R$, $ab \in I \Rightarrow a \in I$ or $b \in I$. For an ideal $I \subset R$ in a ring R we define the factor ring R/I by:

$R/I = \{a + I \mid a \in R\}$ where $a + I := \{a + b \mid b \in I\}$

In fact, $R/I = R/\sim$ where $\sim$ is the

equivalence relation $a \sim b$ iff $a - b \in I$ (it is easy to see that $\sim$ is an equivalence). We define operations $+$ and $\cdot$ on R/I by:

$$(a+I) + (b+I) := (a+b) + I$$



not an operation, just part of the symbol denoting $\{a+b \mid b \in R\}$, ... and

$$(a+I) \cdot (b+I) := a \cdot b + I$$

(multipl. in R; new defined multipl. in R/I)

For these new operations $+$ and $\cdot$ on R/I to make a sense, they have to be independent on the selection of representatives of the equivalence classes in R/I. Due to the fact that I is an ideal in R, they are independent in this way and I (the ideal) show it next time. See you in 2 ~~next~~ weeks (~~next Monday~~ is Easter Monday).