(L 11) (March 30, 2020) For integers d, $0 \le d \le m$

(We set $inj_d(G,H) = \sum_{D \subseteq E, |D|=d} inj_D(G,H)$.

We $\sum$ over all sets $D \subseteq E$ with $|D|=d$ and get that

the last equalities in the last lecture

$$inj_d(G,H) = \sum_{\substack{B \subseteq E \\ |B| \ge d}} (-1)^{|B|-d} \binom{|B|}{d} inj((V,B),H). \quad (*)$$

(Here the binom. coeff. counts d-elem. subsets D in a fixed set $B = D \cup A$. If we replace G with H we get a similar equality

$$inj_d(H,\bar{H}) = \sum_{\substack{B \subseteq F, \\ |B| \ge d}} (-1)^{|B|-d} \binom{|B|}{d} inj((V,B),H). \quad (**)$$

By the lemma $\boxed{\cdots}$ on p. 2 of the previous lecture

(we have a bijection

$$\gamma : \{B \subseteq E \mid d \le |B| < m\} \to \{B \subseteq F \mid d \le |B| < m\}$$

s.t. always $(V,B) \cong (V,\gamma(B))$. Indeed, for any fixed $A \subseteq E$, $A \neq E$, we can pair A-copies in (V,E) with those in (V,F) because their numbers are equal. Then, trivially, always $|B| = |\gamma(B)|$ and

$inj((V,B),H) = inj((V,\delta(B)),H)$. Thus except for the last terms with $B=E$ and $B\neq E$, the summands on the RHS's of (*) and (**) coincide and differ only by order. We subtract (*) and (**) and get:

$$ind_d(G,\bar{H}) - ind_d(H,\bar{H}) = (-1)^{m-d}\binom{m}{d}(inj(G,H) - inj(H,H)).$$

We assume (for contradiction) that $G \not\cong H$. Then $inj(G,H)=0$ (G and H have the same # of edges and an isomorphism between them is the same thing as an injective homomorphism. Always $inj(H,H)\geq 1$

Problem 11.1 Why $inj(H,H)\geq 1$?

thus $|inj_d(G,H) - inj_d(H,\bar{H})| \geq \binom{m}{d}$.

We $\sum$ over $d=0,1,\dots,m$ and use the binomial theorem for $(1+1)^m = m$:

$$2^m = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{m} \leq \sum_{d=0}^{m} |inj_d(G,H) - inj_d(H,\bar{H})| \leq$$

$\leq 2 \cdot n!$

the last inequality follows from the

triangle inequality for $|\cdot|$ and from the equalities $\sum_{d=0}^{n} \binom{n}{d} j_d(G,\vec{H}) = \sum_{d=0}^{n} \binom{n}{d} j_d(H,\vec{H}) = n!$.

Problem 11.2. Why do these equalities hold?

Lemma (Problem 11.3) Proving by induction on $n \in \mathbb{N}$ that for every $n \geq 6$, $n! < \left(\frac{n}{2}\right)^n$. Then we get the inequality $2^n \leq 2 \cdot n! < 2\left(\frac{n}{2}\right)^n$, $n \geq 6$, which under application of the binary log turns in $n < 1 + n(\log_2 n - 1)$, which contradicts the assumed bound $n \geq 1 + n(\log_2 n - 1)$. So $G \cong H$. ☒

I will now jump into the Chapter IV. 9.4 of the LN of Prof. Peltr and will show you some interesting connections between commutative Algebra and Combinatorics. Eventually I will deduce a formula for the number of irreducible Polynomials

in $\mathbb{Z}_p[x]$ (polynomials with coeffs-s in the finite field with p elements, where p is a prime number) with degree $d \in \mathbb{N}$. This formula shows that, in particular, there is always ≥ 1 such polynomial, and we use it to obtain a finite field with p^d elements.

But first I have to review terminology and notions relating to rings and fields.

A (commutative unital) ring is an algebra $R = (R, 0_R, 1_R, +, \cdot)$ (this notation is not in complete accord with ch. IV but I will use it) such that: $0_R \neq 1_R$ are elements of the set R which are neutral to the respective binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$. Both operations $+$ and $\cdot$ are commutative and associative.

Above the adjectives in: mean that the "multiplication" $\cdot$ is comm. and has the neutral element 1_R. Further, the distributive law holds: $\forall a,b,c \in R : a \cdot (b+c) = a(b+c) = (ab) + (ac) =$

$= ab + ac$. Here the symbol for the operation $\cdot$ is (as usual) omitted (we write ab instead of $a \cdot b$) and we omit the brackets ( ) using the convention that $\cdot$ has precedence over $+$. Finally, for every $a \in R$ there is in R an additive inverse $b \in R$, an element satisfying $a + b = 0_R$. We write $-a$ for b: $a + (-a) = 0_R$. This is the definition of a ring. An example is the ring of integers $\mathbb{Z} = (\mathbb{Z}, 0, 1, +, \cdot)$ where 0 and 1 are what they are and $+$ and $\cdot$ are the usual addition and multiplication of integers, respectively. Another example is $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$, the ring of residue classes (of the integers) modulo 6:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

and:

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1 = 1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}$ is infinite but $\mathbb{Z}_6$ is finite. The only units in $\mathbb{Z}_6$ are $\bar{1}$ and $\bar{5}$.

If $a \in R$ is such that for some $b \in R$ we have $ab = 1_R$ - a is multiplicatively invertible in R - we say that a is a unit in R. Units in any ring are important elements and for an Abelian (commutative) group $U_R = (U_R, 1_R, \cdot)$. For example, the units in $\mathbb{Z}$ are just -1 and 1, and in $\mathbb{Z}_6$ they are just $\bar{1}$ and $\bar{5}$ (as you can see from the 2nd table above). Clearly, 0_R is never a unit. If $U_R = R \setminus \{0_R\}$, i.e. every non-zero element in R is a unit, we say that R is a field. So in a field F every $\neq 0_F$ elements has a multiplicative inverse.

See you next week.