$\exists n!$ distinct permutations

A **permutation** of the set $\{a_1,\dots,a_n\}$ is described by a rule that assigns each element of $\{a_1,\dots,a_n\}$ an element of $\{a_1,\dots,a_n\}$ s.t. assign not any twice.

A **permutation** of a set X is a **bijective** function whose domain and range are X. $\pi: X\to X$ $\therefore \forall x\in X, \exists! x'\in X$ s.t $\pi(x')=x \Rightarrow \pi^{-1}: X\to X$ s.t $\pi^{-1}(x)=x'$.

Identity Permutation of X, $e: X\to X$, $e(x)=x$ $\forall x\in X$. Order of permutations matters $\therefore \pi_2\circ\pi_1 \neq \pi_1\circ\pi_2$. **Def: Abstract Groups**: A group consists of a **set** G with a **composition law** $G\times G\to G$, $(g_1,g_2)\mapsto g_1\cdot g_2$, s.t (i) $\exists e\in G$ s.t $e\cdot g=g\cdot e=g$ $\forall g\in G$; (ii) $\forall g\in G, \exists h\in G$ s.t $g\cdot h=h\cdot g=e$. $h:=e^{-1}$ (inverse of g). (iii) Associative law: $\forall g_1,g_2,g_3\in G$ $g_1\cdot(g_2\cdot g_3)=(g_1\cdot g_2)\cdot g_3$; (iv) If $g_1\cdot g_2=g_2\cdot g_1$ $\forall g_1,g_2\in G \Rightarrow (G,\cdot)$ **abelian**. **Prop:** Let $(G,\cdot)$, (a) $\exists! e\in G$, (b) $\forall g\in G, \exists! g^{-1}$, (c) $g,h\in G \Rightarrow (g\cdot h)^{-1}=h^{-1}\cdot g^{-1}$ (d) $g\in G$. $\therefore (g^{-1})^{-1}=g$; Let $g,h,k\in G$. If $g\cdot h=g\cdot k \Rightarrow h=k$, $h\cdot g=k\cdot g \Rightarrow h=k$. **Def: Order of G**, $\#G=|G|$. **Def:** $g\in G$, $\forall n\geq 1\in\mathbb{N}$, $g^n=\underbrace{g\cdot g\cdots g}_{n\text{-times}}$, the **order of g** is the smallest n s.t $g^n=e$. If $\nexists n$ s.t $g^n=e \Rightarrow$ **g has infinite order**. **Prop:** $g\in G$, $n\geq 1$ s.t $g^n=e$ $\therefore$ **order of g divides n**. **Def:** G **cyclic group** if $\exists g\in G$ s.t. $G=\{\dots,g^{-2},g^{-1},e,g,g^2,g^3,\dots\} \Rightarrow$ **g generator**. If $n\geq 1$, let $\zeta_n=e^{2\pi i/n}\in\mathbb{C}$ $\therefore$ multiplication turns $\{1,\zeta,\zeta^2,\dots,\zeta^{n-1}\}$ into cyclic group of order n. In general, for $n\geq 1$, $C_n=\{e,g,g^2,\dots,g^{n-1}\}$ using composition rule $g^i\cdot g^j=g^{i+j \bmod n}$. **Symmetric Group** S_X of $X:=$ all permutations of X, $\circ :=$ composition of permut. **Def: Group Homomorphisms**: G,G', $\phi: G\to G'$ s.t (i) $\phi(g_1\cdot g_2)=\phi(g_1)\cdot\phi(g_2)$ $\forall g_1,g_2\in G$ (ii) $\phi(e)=e'$ (iii) $\phi(g^{-1})=\phi(g)^{-1}$ $\forall g\in G$. **Def:** G_1,G_2 **isomorphic** if $\exists \phi: G_1\to G_2$ **bijective** $\therefore G_1\cong G_2$, ϕ: **isomorphism**. **Remark**: If $G_1\cong G_2 \Rightarrow \#G_1=\#G_2$, G_1 **abelian** $\Rightarrow G_2$ **abelian**, if $g\in G_1$ of order $n \Rightarrow \exists g'\in G_2$ of order n. **Def:** Let $(G,\cdot)$ A **subgroup** H of G, s.t. $H\subset G$ and $(H,\cdot)$ group. (i) $\forall h_1,h_2\in H$, $h_1\cdot h_2\in H$, (ii) $e\in H$, (iii) $\forall h\in H$, $h^{-1}\in H$. **Ex:** Let $g\in G$ be an element of order n, The **cyclic subgroup** $\langle g\rangle=\{e,g,g^2,\dots,g^{n-1}\}\cong C_n$. If $|g|=\infty \Rightarrow \langle g\rangle\cong\mathbb{Z}$. **Def:** Let $\phi: G\to G'$, $\ker(\phi)\overset{\text{def}}{=}\{g\in G: \phi(g)=e'\}$. **Prop:** $\ker(\phi)$ subgroup of G, ϕ **injective** $\iff \ker\{\phi\}=\{e\}$. **Def:** G group, $H\subset G$ subgroup. $\forall g\in G$ (**left**) **coset** of H attached to g, $gH=\{gh: h\in H\}$. **Prop:** $\#G<\infty$, $H\subset G$. (a) $\forall g\in G$ in some coset of H (b) $\forall g_1,g_2$, $|g_1H|=|g_2H|$ (c) $g_1,g_2\in G$ $\therefore g_1H, g_2H$ satisfy either $g_1H=g_2H$ or $g_1H\cap g_2H=\emptyset$. **Theorem: Lagrange's**. Let $\#G<\infty$, H be a subgroup of G $\Rightarrow$ **$\#G=\#H\cdot$(# of distinct cosets of G in H)** $\therefore$ $\#H$ divides $\#G$. Proof: $\forall g_i\in G$, $g_i\in g_iH$. $\therefore G=\bigsqcup_{i}^{k} g_iH$ (distinct cosets have no elements in common) $\therefore \#G=\sum_{i=1}^{k}\#g_iH$, $\#g_1H=\#g_2H=\dots=\#g_kH$ $\therefore \#G=k\#H$. **Def: Index $(G:H)$** number of distinct cosets of H. $\therefore \#G=(G:H)\#H$. **Corollary**: $\#G<\infty$. $g\in G$ $\therefore$ ($|g|$ divides $\#G$). **Prop:** Let p **prime**, $\#G=p \Rightarrow G\cong C_p$ (**cyclic**). **Theorem:** Let p prime, $\#G=p^2 \Rightarrow G$ **abelian**. **Theorem:** (**Sylow's**) $\#G<\infty$, p prime, suppose that p^n divides $\#G$ for some power $n\geq 1$. $\therefore \exists H\subset G$ subgroup s.t $\#H=p^n$. **Def:** $G_1\times G_2=\{(a,b): a\in G_1, b\in G_2\}$, $(a,b)\cdot(a',b')=(\overset{G_1}{a\cdot a'},\overset{G_2}{b\cdot b'})$ $e\in G_1\times G_2=(e_1,e_2)$, $(a,b)^{-1}=(a^{-1},b^{-1})$. $G_1,\dots,G_n \Rightarrow G_1\times\dots\times G_n=(a_1,\dots,a_n)$, $a_i\in G_i$. **Theorem:** $\#G<\infty$ abelian $\therefore \exists m_1,\dots,m_r\in\mathbb{Z}$ s.t. $G\cong(\mathbb{Z}/m_1\mathbb{Z})\times(\mathbb{Z}/m_2\mathbb{Z})\times\dots\times(\mathbb{Z}/m_r\mathbb{Z})$. **Def:** A **ring** R is a set with **two operations**: $a+b$, $a\cdot b$ s.t. (i) $(R,+)$ **abelian group**, $e=0_R$ (ii) $(R,\cdot)$ **Almost a group** but elements in R are not required to have inverses, $\exists 1_R\in R$ s.t. $1_R\cdot a=a\cdot 1_R=a$ $\forall a\in R$, **Associative law** $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ $\forall a,b,c\in R$; (iii) **Distributive law**: $\forall a,b,c\in R$ $a\cdot(b+c)=a\cdot b+a\cdot c$, $(b+c)\cdot a=b\cdot a+c\cdot a$. (iv) If further $a\cdot b=b\cdot a$ $\forall a,b\in R \Rightarrow R$ **commutative**. **Prop:** (a) $0_R\cdot a=0_R$ $\forall a\in R$, (b) $(-a)\cdot(-b)=a\cdot b$ $\forall a,b\in R$, $(-1_R)\cdot a=-a$; **Def:** R,R' rings, **ring homomorphism** $\phi: R\to R'$ s.t $\phi(1_R)=1_{R'}$, $\phi(a+b)=\phi(a)+\phi(b)$ $\phi(a\cdot b)=\phi(a)\cdot\phi(b)$ $\forall a,b\in R$, $\ker(\phi)=\{a\in R: \phi(a)=0_{R'}\}$, $R\cong R'$ if $\exists \phi: R\to R'$ **bijective**; $\mathbb{Z}/m\mathbb{Z}$ $a\sim b$ if $a-b=km \Rightarrow a\equiv b \pmod m$, $\phi: \mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ $\phi(a)=a \bmod m$. **Subrings**: $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$. **Gaussian Integers**: $\mathbb{Z}[i]\subset\mathbb{C}$, $\mathbb{Z}[i]=\{a+bi: a,b\in\mathbb{Z}\}$, **Polynomials Rings**: $R[x]=\{a_0+a_1x+a_2x^2+\dots+a_dx^d : a_0,a_1,\dots,a_d\in R\}$ **Ex:** $\forall(R,+,\cdot)$, $\exists!\ \phi: \mathbb{Z}\to R$. **Def:** A **field** is a **commutative ring** R s.t $\forall a\neq 0\in R$, $\exists b\in R$ s.t $ab=1_R$. $\forall p\in$ Prime, $\mathbb{Z}/p\mathbb{Z}$ is a field ff. **Definition:** Let R be a commutative ring. $a\in R$ a **zero-divisor** if $(a\neq 0, \exists b\neq 0\ b\in R)$ s.t $ab=0$ $\therefore$ R **integral domain** if it **has no zero-divisors**. $\therefore$ R **an integral domain** if $ab=0 \Rightarrow$ either $a=0$ or $b=0$. $\therefore$ $\forall$ F is an integral domain. Not every integral domain is a Field, but $\forall$ ID is a subring of a field ff. **Prop:** (**Cancellation P. of ID**): A **commutative ring** R has **CPID** if $\forall a,b,c\in R, ab=ac \iff [b=c \text{ or } a=0]$ $\therefore$ A commutative Ring has CP iff R an ID. **Def:** Let R commutative, **Group of units** of $R:=R^*=\{a\in R: \exists b\in R$ s.t $ab=1\}<R$, $a\in R^*$: **units**. **Prop:** $(\{a\in R: a\in R^*\},$ ring multiplication) is a group. **Ex:** $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}: a,b\in\mathbb{Z}\}$, $\#\mathbb{Z}[\sqrt{2}]^*=\infty$, **prop:** R a field iff $R^*=\{a\in R: a\neq 0\}=R\setminus\{0\}$ **Prop:** $m\geq 1\in\mathbb{Z}$ $\therefore (\mathbb{Z}/m\mathbb{Z})^*=\{a \bmod m: \gcd(a,m)=1\}$. **Def:** $R_1,\dots,R_n$ $\therefore R_1\times\dots\times R_n=\{(a_1,\dots,a_n): a_1\in R_1,\dots,a_n\in R_n\}$. Let $R_1,\dots,R_n$ commutative $\Rightarrow$ Unit group of product i.e. $(R_1\times\dots\times R_n)^*\cong R_1^*\times\dots\times R_n^*$. **Def:** R commutative. An **ideal** of R, $I\neq\emptyset$ s.t $I\subseteq R$ (i) If $a\in I$, $b\in I \Rightarrow a+b\in I$. If $a\in I$, $r\in R \Rightarrow ra\in I$. **Def:** R commutative, $c\in R$. The **Principal Ideal generated by c** $:=cR$, is the set of all multiples of c, $cR=(c)=\{rc: r\in R\}$. $\forall R$ has at least ideals $\{0\},\{R\}$ **Remark:** $I\subseteq R$, if $1\in I \Rightarrow \forall r\in R$, $r\cdot 1\in I$ $\therefore I=R$. **Def:** R comm. $I\subseteq R$ $\therefore \forall a\in R$, **coset of a** is the **set** $a+I=\{a+c: c\in I\}$ Given cosets $(a+I)$, $(b+I)$, $(a+I)+(b+I)=(a+b)+I$, $(a+I)\cdot(b+I)=(a\cdot b)+I$. **Collection of distinct cosets**: R/I. **Prop:** R commutative, $I\subseteq R$ (a) $a'+I=a+I$ iff $a'-a\in I$, (b) Addition and mult. of cosets well-defined $\therefore$ **R/I commutative ring**. **Prop:** (a) $I\subseteq R$ $\therefore R\to R/I$ $a\mapsto a+I$ **ring homomorphism** s.t $\ker(\phi)=I$, (b) $\phi: R\to R'$, (i) $\ker(\phi)$ ideal of R, (ii) ϕ injective iff $\ker(\phi)=\{0\}$

Def: $\phi: \mathbb{Z}\to R$ be the unique **homomorphism** determined by the condition $\phi(1)=1_R$. $K\in R(\phi)=I\subset\mathbb{Z}$, $\forall I\subseteq\mathbb{Z}$ is **principal**

∴ ∃! m≥0 s.t $\ker(\phi)=m\mathbb{Z}$, m characteristic of R ∴ $\underbrace{1_R+1_R+\dots+1_R}_{m\text{-times}}=0_R$. $\mathbb{Z}/m\mathbb{Z}$ has characteristic m, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ m=0. Prop: If R has ch. m, ∃ φ injective $\mathbb{Z}/m\mathbb{Z}\hookrightarrow R$. Theorem: Let p prime, R commutative with m=p ∴ $f:R\to R$, $f(a)=a^p$ homomorphism ∴ $\forall a,b\in R$, $n\geq 0$ $(a+b)^{p^n}=a^{p^n}+b^{p^n}$. Def: R comm. $I\subseteq R$ prime ideal if $I\neq R$ and if whenever $ab\in I \Rightarrow$ either $a\in I$ or $b\in I$. ∴ $a\notin I, b\notin I \Rightarrow ab\notin I$

Def: R comm. $I\in R$ Maximal Ideal if $I\neq R$, and if J ideal of R s.t $I\subseteq J\subseteq R \Rightarrow$ either J=I or J=R. Prop: $p\in\mathbb{Z}$ prime ∴ Ideal $p\mathbb{Z}$ prime ideal and Maximal Ideal. Theorem: R commutative, I ideal s.t $I\neq R$ (a) I prime Ideal iff the quotient ring R/I an ID (b) I maximal Ideal iff R/I field. Corollary: Every Maximal ideal is a prime ideal: I maximal $\Rightarrow$ R/I field $\Rightarrow$ R/I ID $\Rightarrow$ I prime.

R domain $\iff \{0\}$ prime ideal in R, R field $\iff \{0\}$ maximal ideal in R. $I\subseteq R$ maximal $\iff$ R/I a field. $\forall\ \varphi:R\to S$ produces an isomorphism from $R/\ker(\phi)\to\mathrm{Im}(\phi)$, $(a+I)\mapsto\varphi(a)$ ∴ $R\to R/\ker(\varphi)\cong\mathrm{Im}(\varphi)\to S$

Def: Let $\mathbb{F}$ field, A vector space with field scalars $\mathbb{F}$ is an abelian group V with addition operation +, and rule of multiplication $v\in V$ times a scalar $c\in\mathbb{F}\Rightarrow cv\in V$. (i) Id. Law: $1v=v\ \forall v\in V$ (ii) Distributive law: $c(v_1+v_2)=cv_1+cv_2\ \forall v_1,v_2\in V, c\in\mathbb{F}$ (iii) Distrib. law $(c_1+c_2)v=c_1v+c_2v\ \forall v\in V, c_1,c_2\in\mathbb{F}$; (iv) Associative law: $(c_1c_2)v=c_1(c_2v)\ \forall v,c_1,c_2$. Id. element $e\in V$, $e=0_v$. Prop: V an $\mathbb{F}$-Vector space (a) $0v=0\ \forall v\in V$ (b) $(-1)v+v=0\ \forall v\in V$. Def: $\mathbb{F}$, V, W, $\mathbb{F}$-vector spaces. A linear Transformation $L:V\to W$ s.t. $L(c_1v_1+c_2v_2)=c_1L(v_1)+c_2L(v_2)\ \forall v_1,v_2\in V, c_1,c_2\in\mathbb{F}$

Ex: $\mathbb{F}$, $n\geq 1$ ∴ $\mathbb{F}^n$ − $\mathbb{F}$-vector space $\mathbb{F}^n=\{(a_1,\dots,a_n): a_1,\dots,a_n\in\mathbb{F}\}$, $(a_1+\dots+a_n)+(b_1+\dots+b_n)=(a_1+b_1,\dots,a_n+b_n)$, $c(a_1,a_2,\dots,a_n)=(ca_1,\dots,ca_n)$. Ex: $\mathbb{F}[x]$ with coefficients in $\mathbb{F}$, we add and multiply polynomials by scalars. $\forall a\in\mathbb{F}$, evaluation map $E_a:\mathbb{F}[x]\to\mathbb{F}$, $E_a(f(x))=f(a)$. More generally $\forall a_1,\dots,a_n\in\mathbb{F}$, define lin. t. $E_a:\mathbb{F}[x]\to\mathbb{F}^n$, $E_a(f(x))=(f(a_1),\dots,f(a_n))$. Ex: $V=\{f:\mathbb{R}\to\mathbb{R}\}$, $V=\{\text{continuous } f:\mathbb{R}\to\mathbb{R}\}$ (cont), $V=\{\text{diff. } f:\mathbb{R}\to\mathbb{R}\}$ (diff) $\mathbb{R}$-Vector Spaces: $(f+g)(x)=f(x)+g(x)$, $(cf)(x)=cf(x)$. Def: V $\mathbb{F}$-Vector S. A finite basis for V is a finite set of vectors $\beta=\{v_1,\dots,v_n\}\subset V$ s.t $\forall v\in V$, $v=a_1v_1+a_2v_2+\dots+a_nv_n$ ∃! $a_1,\dots,a_n\in\mathbb{F}$. $a_1v_1+\dots+a_nv_n$ linear Combination of $v_1,\dots,v_n$. Ex: $\mathbb{F}$, standard basis is the collection of vectors $\{e_1,e_2,\dots,e_n\}$, where $e_k=(0,0,\dots,\underset{k\text{-th}}{1},\dots,0)$ ∴ $v=(a_1,\dots,a_n)\in\mathbb{F}^n=a_1e_1+\dots+a_ne_n$. Def: V, let $\mathcal{A}=\{v_1,\dots,v_n\}$ be a finite set of vectors. (i) $\mathcal{A}$ spans V if $\forall v\in V$, $\exists a_1,\dots,a_n\in\mathbb{F}$ s.t $v=a_1v_1+\dots+a_nv_n$ ∴ Span($\mathcal{A}$) = $\langle\mathcal{A}\rangle=\{a_1v_1+\dots+a_nv_n: a_1,\dots,a_n\in\mathbb{F}\}$. $\mathcal{A}$ spans V if Span($\mathcal{A}$)=V. (ii) $\mathcal{A}$ lin. independent if the only scalars $a_1,\dots,a_n\in\mathbb{F}$ that make $a_1v_1+\dots+a_nv_n=0\Rightarrow a_1=a_2=\dots=a_n=0$. $\mathcal{A}$ a basis for V iff $\mathcal{A}$ lin. ind. and Span($\mathcal{A}$)=V. Theorem: V, $\mathbb{F}$. $S\subset V$ s.t Span(S)=V. Let $\mathcal{L}\subseteq S$ s.t $\mathcal{L}$ lin. ind. ∴ ∃ β_V basis s.t $\mathcal{L}\subseteq\beta\subseteq S$

Theorem: V a vector space with finite basis $\beta_V\Rightarrow\forall\ \beta_{iV}$, $\#\beta_{iV}=\#\beta_{jV}$. Def: Dim(V) = $\#\beta_{iV}\ \forall i$., if Dim(V)=∞ V infinite-dimensional. Lemma: V, $\mathbb{F}$. Let S be a finite set of vectors in V s.t Span(S)=V. Let $\mathcal{L}$ be a set of vectors lin. ind. ∴ $\forall v\in\mathcal{L}\setminus S$, $\exists w\in S\setminus\mathcal{L}$ s.t Span$[(S\setminus\{w\})\cup\{v\}]=V$ ∴ We can swap an $\mathcal{L}$ vector not in S for an S vector not in $\mathcal{L}$ while preserving spanning. Lemma: Let V be an $\mathbb{F}$ vector space. $S\subset V$ s.t Span(S)=V, $\mathcal{L}\subset V$ lin. ind set ∴ $\#\mathcal{L}\leq\#S$. $f:X\to Y$ bijective if f both injective and surjective

$f:X\to Y$ injective if $\forall a,b\in X$, $f(a)=f(b)\Rightarrow a=b$. ∴ if $a\neq b\Rightarrow f(a)\neq f(b)$, $f:X\to Y$ surjective if $\forall y\in Y$, $\exists x\in X$ s.t $f(x)=y$ fog injective if f,g are injective; fog surjective if both f,g surjective ∴ fog surjective if f,g b. and inj. Given maps $f:X\to Y$ $g:Y\to X$ are inverses if $fog:Y\to Y$ and $gof:X\to X$ are id. maps ey, ex. If $\exists f^{-1}$ ∴ f bijective. Let X, Y finite sets, #X=m, #Y=n. If $m>n\Rightarrow f:\underset{(m)}{X}\to\underset{(n)}{Y}$ cannot be injective (∴ f injective $\Rightarrow m\leq n$); If $m<n$: f not surjective (∴ f surjective $\Rightarrow m\geq n$ ∴ $m\neq n$ f not bijective. If $f:X\to X$ either injective or surjective (X finite) $\Rightarrow$ f bijective. Theorem: If $S=\{v_1,\dots,v_n\}$ spanning set of V, $\exists\ \beta\subseteq S$ s.t β a basis of V. Theorem: If Span(S)=V, $I\subset S$ lin. ind. set in V $\Rightarrow$ ∃ basis β s.t $I\subset\beta\subset S$. Def: A field: commutative ring s.t $\forall a\neq 0\in\mathbb{F}$ $\exists b\in\mathbb{F}$ s.t $ab=1$. Def: R comm. ring. (Unit Group) $R^*=\{a\in R: \exists b\in R \text{ s.t } ab=1\}$ ∴ $\mathbb{F}^*=\{a\in\mathbb{F}: a\neq 0\}=\mathbb{F}\setminus\{0\}$. Prop: $\mathbb{F}$, $\mathbb{K}$ fields, $\phi:\mathbb{F}\to\mathbb{K}$ ring hom. (i) ϕ injective (ii) $a\in\mathbb{F}^*\Rightarrow\phi(a^{-1})=\phi(a)^{-1}$. Ex: $\mathbb{Q}(i)=\{a+bi: a,b\in\mathbb{Q}\}$, $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}: a+b\in\mathbb{Q}\}$. $\mathbb{Z}/m\mathbb{Z}$ need not be a field $\mathbb{Z}/p\mathbb{Z}$ a field if p prime: $\mathbb{F}_p$. $\forall p^k$ ∃! $\mathbb{F}$ s.t. $\#\mathbb{F}=p^k$. Subfield $\mathbb{F}\subset\mathbb{K}$ a field using $(+,\cdot)$ from $\mathbb{K}$. ($\mathbb{K}$ extension of $\mathbb{F}$: $\mathbb{K}/\mathbb{F}$)

prop: Let $\mathbb{L}/\mathbb{F}$ an extension of fields, Let $\alpha_1,\dots,\alpha_n\in\mathbb{L}$ ∴ ∃! $\mathbb{K}$ s.t. (i) $\mathbb{F}\leq\mathbb{K}\leq\mathbb{L}$, (ii) $\alpha_1,\dots,\alpha_n\in\mathbb{K}$ (iii) If $\mathbb{K}'$ a field s.t $\mathbb{F}\leq\mathbb{K}'\leq\mathbb{L}$ $\alpha_1,\dots,\alpha_n\in\mathbb{K}'\Rightarrow\mathbb{K}\leq\mathbb{K}'$. Def: $\mathbb{K}/\mathbb{F}$ extension of fields. The degree of $\mathbb{K}$ over $\mathbb{F}$: $[\mathbb{K}:\mathbb{F}]=\dim_{\mathbb{F}}(\mathbb{K})$. Ex: $[\mathbb{Q}(i):\mathbb{Q}]=2$ since $\{1,i\}$ is a $\mathbb{Q}$ basis for $\mathbb{Q}(i)$, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, since $\{1,\sqrt{2}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2})$, $[\mathbb{C}:\mathbb{R}]=2$, $\{1,i\}$ $\mathbb{R}$-basis $\mathbb{C}$ $[\mathbb{R}:\mathbb{Q}]=\infty$. Theorem: $\mathbb{L}/\mathbb{K}/\mathbb{F}$: (a) if $[L:K],[K:F]<\infty\Rightarrow[L:F]=[L:K]\cdot[K:F]$ if $[L:K]\ v\ [K:F]=\infty\Rightarrow[L:F]=\infty$. Def: $\mathbb{F}$ field, let $f(x)\in\mathbb{F}[x]$ be a non-zero polynomial $f(x)=a_0+a_1x+\dots+a_dx^d$, $a_d\neq 0$ ∴ $\deg(f)=d$. $f_1(x),f_2(x)\in\mathbb{F}[x]\Rightarrow\deg(f_1f_2)=\deg(f_1)+\deg(f_2)$ Prop: $\mathbb{F}$, $f(x),g(x)\in\mathbb{F}[x]$, $g(x)\neq 0$ ∴ ∃! $q(x),r(x)\in\mathbb{F}[x]$ s.t. $f(x)=g(x)q(x)+r(x)$, $\deg(r)<\deg(g)$. Def: An ideal I in R principal if $\exists c\in R$ s.t $I=\{cr: r\in R\}$. Theorem: $\mathbb{F}$, $I\leq\mathbb{F}[x]$ ideal in the

③

ring $\mathbb{F}[x]$ ∴ I principal. **Def:** $\mathbb{F}$, non-constant $f(x)\in\mathbb{F}[x]$ reducible (over $\mathbb{F}$) if $\exists$ non-constant $g(x),h(x)\in\mathbb{F}[x]$ s.t. $f(x)=g(x)h(x)$. ∴ $x^2-1=(x+1)(x-1)$ i.e. reducible in $\mathbb{Q}[x]$. $x^2+1=(x+i)(x-i)\Rightarrow$ reducible in $\mathbb{Q}(i)[x]$. $\forall f(x)$ s.t $\deg(f)=1\Rightarrow$ irreducible. if $f(x)\in\mathbb{F}[x]$, $\deg(f)=2\vee3\Rightarrow f(x)$ irreducible in $\mathbb{F}[x]\Leftrightarrow\nexists$ roots of $f(x)$ in $\mathbb{F}$. **Theorem:** $f(x)\neq0\in\mathbb{F}[x]$: TFAE (i) $f(x)$ irreducible (ii) principal ideal $f(x)\mathbb{F}[x]$ generated by $f(x)$ is maximal (iii) $\mathbb{F}[x]/f(x)\mathbb{F}[x]$ a field. **Theorem:** $\mathbb{F}$ field, let $f(x)\in\mathbb{F}[x]$ irreducible. set $I_f=f(x)\mathbb{F}[x]$ principal ideal gen.by $f(x)$, let $K_f=\mathbb{F}[x]/I_f$ quotient ring. (a) K_f is a field (b) We may identify the field $\mathbb{F}$ with a subfield of K_f via $\mathbb{F}\longrightarrow K_f$ s.t $c\mapsto c+I_f$ (c) $f(x)$ $\exists$ root in field K_f (d) Field K_f finite extension of $\mathbb{F}$. ∴ $[K_f:\mathbb{F}]=\deg(f)$. **Def:** Let R ring $\phi:\mathbb{Z}\to R$ be the unique hom. s.t. $\phi(1)=1_R$. $\ker(\phi)$ ideal of $\mathbb{Z}$ (every ideal of $\mathbb{Z}$ principal) ∴ $\exists!\, m\geq0\in\mathbb{Z}$ s.t. $\ker(\phi)=m\mathbb{Z}$: m "characteristic" of R. $m:=$ smallest s.t. $\underbrace{1_R+1_R+\dots+1_R}_{m\text{-times}}=0_R$. **Prop:** $\mathbb{F}$ finite field (i) characteristic of $\mathbb{F}$ prime (ii) let $p=\mathrm{char}(\mathbb{F})$ ∴ $\mathbb{F}_p$ subfield of $\mathbb{F}$ s.t. $\exists!$ injective homomorphism $\mathbb{F}_p\hookrightarrow\mathbb{F}$ (iii) $\#\mathbb{F}=p^{[\mathbb{F}:\mathbb{F}_p]}$ $\Rightarrow\#\mathbb{F}$ (finite) $=p^k$. **Theorem:** p prime, $d\geq1$ ∴ ring $\mathbb{F}_p[x]$ contains an irreducible polynomial of degree d. **Theorem:** p prime, $d\geq1$ (i) $\exists\,\mathbb{F}$ containing p^d elements (ii) $\forall\,\mathbb{F},\mathbb{F}'$ s.t. $\#\mathbb{F}=\#\mathbb{F}'\Rightarrow\mathbb{F}\cong\mathbb{F}'$. **Def:** $\mathbb{G}$ group, $H\leq\mathbb{G}$ (subgroup). $\forall g\in\mathbb{G}$ gives a left coset $gH=\{gh:h\in H\}$. **Def:** $H\leq\mathbb{G}$. Set of left cosets $\mathbb{G}/H=\{$(left) cosets of $H\}$. Let $C_1,\dots,C_k$ distinct cosets of H. (ii) $\forall g\in\mathbb{G}$ $g\in C_i$, $\#C_i=\#C_j$ $\forall i,j$. (iii) $g_1,g_2\in\mathbb{G}$ ∴ g_1H, $g_2H\Rightarrow$ $g_1H=g_2H\ \vee\ g_1H\cap gH_2=\emptyset$ ∴ $\mathbb{G}=C_1\sqcup C_2\sqcup\dots\sqcup C_k$, $C=gH\Leftrightarrow g\in C$. **Def:** $H\leq\mathbb{G}$. $\forall g\in\mathbb{G}$ the g-conjugate of $H:=g^{-1}Hg=\{g^{-1}hg:h\in H\}$ H normal-subgroup if $g^{-1}Hg=H$ $\forall g\in\mathbb{G}$ ∴ $\mathbb{G}$ abelian $\Rightarrow\forall H\leq\mathbb{G}$ normal. **Prop:** $\phi:\mathbb{G}\to\mathbb{G}'$ (group-homomorphism) $\Rightarrow\ker(\phi)$ normal subgroup of $\mathbb{G}$. **Prop:** $H\subset\mathbb{G}$ (i) If $g^{-1}Hg\leq H$ $\forall g\in\mathbb{G}\Rightarrow H$ normal-subgroup of $\mathbb{G}$ (ii) $\forall g\in H$, $g^{-1}Hg$ subgroup of $\mathbb{G}$ (iii) $\forall g\in\mathbb{G}$, the map $H\to g^{-1}Hg$ defined $h\mapsto g^{-1}hg$ is a group isomorphism. **Lemma:** $H\leq\mathbb{G}$ normal-subgroup. Suppose $g_1,g_1',g_2,g_2'\in\mathbb{G}$ satisfy $g_1'H=g_1H\wedge g_2'H=g_2H\Rightarrow$ $g_1'g_2'H=g_1g_2H$. **Theorem:** $H\leq\mathbb{G}$ normal-subgroup (i) Collection of cosets $\mathbb{G}/H$ is a group via $g_1H\cdot g_2H=g_1g_2H$ (ii) $\phi:\mathbb{G}\to\mathbb{G}/H$, $\phi(g)=gH$ is a homomorphism s.t. $\ker(\phi)=H$ (iii) Let $\psi:\mathbb{G}\to\mathbb{G}'$ (homomorphism) s.t. $H\leq\ker(\psi)\Rightarrow\exists!$ homomorphism $\lambda:\mathbb{G}/H\to H'$ s.t $\lambda(gH)=\psi(g)$ (iv) Take $H=\ker(\psi)$ in (iii) $\Rightarrow\lambda:\mathbb{G}/\ker(\psi)\longrightarrow\mathbb{G}'$ injective ∴ $\lambda:\mathbb{G}/\ker(\psi)\xrightarrow{\text{isomorphism}}\mathrm{Image}(\lambda)\leq\mathbb{G}'$. **Def:** $\mathbb{G}$ group, X set. An action $\mathbb{G}$ on X is a rule that assigns each element $g\in\mathbb{G}$ and each $x\in X$ another element $g\cdot x\in X$ s.t. (i) Id. Axiom: $e\cdot x=x$ $\forall x\in X$ (ii) Associative Axiom: $(g_1g_2)\cdot x=g_1\cdot(g_2\cdot x)$ $\forall x\in X$, $g_1,g_2\in\mathbb{G}$. **Def:** Given a group $\mathbb{G}$ acting on X (set) $\forall x\in X$ determines: (i) The orbit of x (elements of X to which x is sent to by action of $\mathbb{G}$) Orbit: $\mathbb{G}x=\{g\cdot x:g\in\mathbb{G}\}$ (ii) Stabilizer (elements of $\mathbb{G}$ that leave x unchanged) Stabilizer: $\mathbb{G}_x=\{g\in\mathbb{G}:g\cdot x=x\}$ **Prop:** $\mathbb{G}$ group acts on X (i) $x\in X$, stabilizer $\mathbb{G}_x$ subgroup of $\mathbb{G}$ (ii) Define a relation $\sim$ on X s.t. $x\sim y$ if $y=gx$ for some $g\in\mathbb{G}$ ∴ $\sim$ (equivalence relation) $\Rightarrow$ (equivalence class of x) $=\mathbb{G}x$ (orbit of x) (iii) $\exists$ well-defined bijection $\alpha:\mathbb{G}/\mathbb{G}_x\longrightarrow\mathbb{G}x$ s.t. Input: Coset (C) of subgroup $\mathbb{G}_x$, Computation Choose $g\in\mathbb{G}$. Output: $\alpha(C)$ is the element $g\cdot x\in\mathbb{G}x$. In particular, if $\mathbb{G}$ finite $\Rightarrow\#\mathbb{G}x=\frac{\#\mathbb{G}}{\#\mathbb{G}_x}$. Equivalence class of $x\in X$: $\{y\in X:x\sim y\}=\{y\in X:y=gx$ for some $g\in\mathbb{G}\}=\{gx:g\in\mathbb{G}\}=\mathbb{G}x$. **Def:** $\mathbb{G}$ acts transitively on X if $\mathbb{G}x=X$ $\forall x\in X$. **Orbit-Stabilizer Theorem:** Let $\mathbb{G}$ finite group acting on finite set X. Choose $x_1,\dots,x_k\in X$ s.t. $\mathbb{G}x_1,\dots,\mathbb{G}x_k$ are the distinct orbits of elements of X. ∴ $\#X=\sum_{i=1}^{k}\#\mathbb{G}x_i=\sum_{i=1}^{k}\frac{\#\mathbb{G}}{\#\mathbb{G}_{x_i}}$. **Def:** Center of $\mathbb{G}$ ($Z(\mathbb{G})$) set of elements in $\mathbb{G}$ that commute with every element of $\mathbb{G}$, $Z(\mathbb{G})=\{g\in\mathbb{G}:gg'=g'g\ \forall g'\in\mathbb{G}\}$ (normal subgroup) **Theorem:** p prime. Let $\#\mathbb{G}=p^n$ ($n\geq1$) $\Rightarrow Z(\mathbb{G})\neq\{e\}$ i.e. $\exists h\in\mathbb{G}$ s.t. $\forall g\in\mathbb{G}$ $hg=gh$. **Corollary:** p prime, $\#\mathbb{G}=p^2\Rightarrow\mathbb{G}$ abelian. **Def:** $\mathbb{G}$ group, $H\leq\mathbb{G}$. The centralizer of H: $Z_{\mathbb{G}}(H)$ set of elements of $\mathbb{G}$ that commute $\forall h\in H$ $Z_{\mathbb{G}}(H)=\{g\in\mathbb{G}:gh=hg\ \forall h\in H\}$ **Def:** $H\leq\mathbb{G}$. Normalizer of H: $N_{\mathbb{G}}(H)=\{g\in\mathbb{G}:g^{-1}Hg=H\}$ ∴ $N_{\mathbb{G}}(H)=\mathbb{G}\Leftrightarrow H$ normal-subgroup of $\mathbb{G}$. **Sylow's Theorem I:** $\mathbb{G}$ finite group, p prime, let p^n largest power of p that divides $\#\mathbb{G}\Rightarrow\exists H\leq\mathbb{G}$ s.t. $\#H=p^n$. **Lemma:** $p,n\geq0,m\geq1$ s.t. $p\nmid m\Rightarrow p\nmid\binom{p^nm}{p^n}$. **Definition:** $\mathbb{G}$ finite, p prime, let p^n largest s.t. $p^n\mid\#\mathbb{G}$. A subgroup $H\leq\mathbb{G}$ s.t $\#H=p^n$ called p-Sylow subgroup. $\mathbb{G}$ has at least one Sylow subgroup. **Remark:** If $p^r\mid\#\mathbb{G}$, $\exists H\leq\mathbb{G}$ s.t $\#H=p^r$ even if p^r is not the largest dividing $\#\mathbb{G}$. If $p\neq q$ primes s.t. $p,q\mid\#\mathbb{G}$ take p-Sylow H_p, q-Sylow H_q : $H_p\cap H_q=\{e\}$. **Remark:** If $p_1,\dots,p_r\mid\#\mathbb{G}$ distinct primes $\Rightarrow p$-Sylow subgroups of $\mathbb{G}$ are large, $\#\mathbb{G}=\#H_{p_1}\cdot\#H_{p_2}\cdot\dots\cdot\#H_{p_r}$. **Sylow's Theorem:** $\mathbb{G}$ finite group, p prime. (i) $\mathbb{G}$ has at least one p-Sylow subgroup i.e. $\exists H\leq\mathbb{G}$ s.t. $\#H=p^n$, p^n largest s.t. $p^n\mid\#\mathbb{G}$ (ii) Let H_1,H_2 p-Sylow $\leq\mathbb{G}$ $\Rightarrow H_1,H_2$ are conjugate i.e. $\exists g\in\mathbb{G}$ s.t. $H_2=g^{-1}H_1g$ (iii) Let H p-Sylow, $\kappa=\#$ distinct p-Sylow subgroups of $\mathbb{G}\Rightarrow\kappa\mid\#\mathbb{G}\wedge\kappa\equiv1\ \mathrm{mod}(p)$. **Lemma:** $\mathbb{G}$ fin. group, $H\leq\mathbb{G}\Rightarrow$ H has exactly $\#\mathbb{G}/\#N_{\mathbb{G}}(H)$ distinct conjugates in $\mathbb{G}$. $\mathrm{Conj}(H)=\{$subgroups of $\mathbb{G}$ conjugate to $H\}$. **Lemma:** Let D fin. group, let $A\leq D$, $B\leq D$, let $AB=\{ab:a\in A,b\in B\}$ $\#AB=\frac{\#A\cdot\#B}{\#(A\cap B)}$. **Sylow's Theorem:** $\mathbb{G}$ finite, p prime (a) $\mathbb{G}$ has at least one p-sylow subgroup $\#H=p^n$, $p^n\mid\#\mathbb{G}$ (b) all p-sylow subgroups of $\mathbb{G}$ are conjugate of each other i.e. H_1,H_2 are p-Sylow subgroups of $\mathbb{G}\Rightarrow\exists g\in\mathbb{G}$ s.t. $H_2=g^{-1}H_1g$ (c) $H_1,\dots,H_\kappa$ distinct p-Sylow subgroups of $\mathbb{G}$ ∴ (i) $\kappa=\#\mathbb{G}/\#N_{\mathbb{G}}(H_1)$ so $\kappa\mid\#\mathbb{G}$ (ii) $\kappa\equiv1\ (\mathrm{mod}\,p)$. **Def:** R ring, $u\in R$ unit if $\exists b\in R$ s.t. $ab=1$. If $u\in R^*\Rightarrow\forall a\in R$ $a=u^{-1}u\cdot a$. **Def:** R, $a\neq0\in R$ irreducible if $a\notin R^*$ and only factorization of $a=bc$ s.t. $bvc\in R^*$. **Def:** $a,b\in R$, $b\neq0$. We say b divides a ($b\mid a$)

④

if $\exists c \in R$ s.t. $a = bc$ $\therefore b|a \iff a \in bR$ (ideal) $\iff aR \subseteq bR$ Def: R I.D. (i.e.) commutative ring with no zero-divisors

$\therefore R$ is a unique factorization domain (UFD) if: (i) $a \neq 0 \notin R^*$ $\therefore a = b_1 \cdot b_2 \cdot \ldots \cdot b_n$ using irreducible elements $b_1, b_2, \ldots, b_n \in R$

(ii) Suppose $b_1, b_2, \ldots, b_n \in R$, $c_1, \ldots, c_n \in R$ irreducible elements. Suppose further $b_1 \cdots b_n = c_1 \cdots c_m \Rightarrow m = n$, $\exists u_1, \ldots, u_n \in R^*$ s.t. $c_1 = u_1 b_1, \ldots, c_n = u_n b_n$

Permutation Groups: A permutation of a set X is a bijective function $\pi: X \to X$ and the set of permutations S_X forms a group where group law is composition of functions. Def: The group of permutations of $\{1, 2, \ldots, n\} := S_n$. Prop: $\# S_n = n!$ (ii) $\forall n \geq 3$ S_n non-abelian. A permutation $\pi \in S_n$ determined by what it does to each of $1, 2, \ldots, n$ $\therefore \pi(1)$: n options, $\pi(2)$: $(n-1)$, ..., $\pi(n)$: 1 $\therefore \exists n!$ possibilities for π. Def: Let $\pi \in S_n$, suppose that the π-orbit of a contains k elements $\therefore$ orbit: $(a, \pi(a), \pi^2(a), \ldots, \pi^{k-1}(a))$. Def: A group $\mathcal{G}$ is a simple group if its only normal subgroups are $\mathcal{G}, \{e\}$

Ex: An abelian group $\mathcal{G}$ simple iff it is cyclic of prime order. Follows from: $\forall$ subgroups of an abelian are normal. $\forall g \neq e \in \mathcal{G} \Rightarrow \langle g \rangle = \mathcal{G}$. $\therefore \mathcal{G}$ cyclic say $\mathcal{G} = C_n$. C_n has subgroups of order m $\forall m | n$ $\therefore m = 1, n \Rightarrow n$ prime. Ex: Let p^k (prime powers), $\#\mathcal{G} = p^k$. $\mathcal{G}$ simple iff $k = 1$. By theorem $\mathcal{G}$ has a non-trivial center $Z(\mathcal{G}) \neq \{e\}$. The center is a normal subgroup $\therefore \mathcal{G}$ simple $\rightarrow \mathcal{G} = Z(\mathcal{G}) \Rightarrow \mathcal{G}$ abelian $\therefore \#\mathcal{G} = p^1 = p$. Homomorphisms from $\mathbb{Z}$ to a group: $\mathcal{G}$ group, $x \in \mathcal{G}$, define $x^n \in \mathcal{G}$ $\forall n \in \mathbb{Z}$ $\therefore x^{m+n} = x^m x^n$ i.e. $\forall x \in \mathcal{G}$ the map that takes $n \xrightarrow{\phi} x^n$ (homomorphism). Theorem: $\forall \mathcal{G}$ group, $\forall x \in \mathcal{G}$, $\exists! \phi_x: \mathbb{Z} \to \mathcal{G}$ s.t. $\phi_x(1) = x$ $\therefore \exists$ bijection between the set $\mathcal{G}$ and the set of all homomorphisms $\mathbb{Z} \to \mathcal{G}$. $x^{mn} = (x^m)^n$ $\forall \mathcal{G}$, $\forall x \in \mathcal{G}$, $\forall m, n \in \mathbb{Z}$. Proof: Compose the map ϕ_n with the map $\mathbb{Z} \to \mathbb{Z}$ that multiplies by m. (i.e. composition of homomorphisms). This composed map takes $1 \to \phi_x(m) = x^m$ $\mathbb{Z} \to \mathcal{G}$ $1 \mapsto x^m$ $\therefore \phi_{x^m}(n) \to (x^m)^n$. If $\mathcal{G}$ group $\exists$ "smallest subgroup of $\mathcal{G}$ containing S" $:= \langle S \rangle$ (intersection of all subgroups of $\mathcal{G}$ containing S)

Def: $\mathcal{G}$ cyclic if $\exists x \in \mathcal{G}$ s.t. $\langle x \rangle = \mathcal{G}$ $\therefore \langle x \rangle$ cyclic group. $\mathcal{G}$ cyclic iff $\exists$ surjective group homomorphism $\mathbb{Z} \xrightarrow{\phi} \mathcal{G}$ $\ker(\phi) \leq \mathbb{Z}$ (always)

Subgroups of $\mathbb{Z}$: $\{0\}$, $\forall m > 0$ $\{m\mathbb{Z}\}$. Let $\phi_x: \mathbb{Z} \to \mathcal{G}$ if $\ker(\phi_x) = \{0\} \Rightarrow \phi_x$ injective: It gives an isomorphism from $\mathbb{Z}$ to $\langle x \rangle$ if $\ker(\phi_x) = m\mathbb{Z} \Rightarrow \phi_x$ gives an isomorphism from $\mathbb{Z}/m\mathbb{Z} \to \langle x \rangle$. $\therefore \forall$ cyclic group $\cong \mathbb{Z}$ v $\mathbb{Z}/m\mathbb{Z}$, $\forall$ ring R, $\exists!$ $\phi: \mathbb{Z} \xrightarrow{hom} R$.

Cosets: $\mathcal{G}$ a group $H \leq \mathcal{G}$ subgroup $\therefore \forall a \in \mathcal{G}$ define the subset aH (left) coset of H determined by a. $aH = \{ah : h \in H\}$. Just if $x \in aH$. $x \in aH \iff \exists h \in H$ s.t. $x = ah \iff \exists h \in H$ s.t. $h = a^{-1}x \iff a^{-1}x \in H$. $\forall g \in \mathcal{G}$ belongs to only one left coset of H: $\forall a \in \mathcal{G}$, $a \in aH$ $\therefore a \in xH \Rightarrow aH = xH$ $\therefore x, y \in \mathcal{G}$ belong to the same left coset iff $x^{-1}y \in H$ v $y^{-1}x \in H$. Right Cosets: $H \to Ha$. $\forall g \in \mathcal{G}$ $\in$ only one (right) coset. $x, y \in$ (right) coset iff $xy^{-1} \in H$ v $yx^{-1} \in H$. H normal $\iff aH = Ha$ $\forall a \in \mathcal{G}$. In general, $\forall$ (right) coset of H is a (left) coset of some other subgroup: $Ha = a(a^{-1}Ha)$.

Orbits: When $\mathcal{G}$ acts on a set X, $\forall x \in X$ define $\mathcal{G}x \subseteq X: \{g \cdot x : g \in \mathcal{G}\}$, As with cosets, $\forall x \in X$ belongs to only one orbit: $x \in \mathcal{G}x$, if $x \in \mathcal{G}y \Rightarrow \mathcal{G}x = \mathcal{G}y$. When $\mathcal{G}$ acts on a set X, $\forall x \in X$ $\exists$ subgroup $G_x \leq \mathcal{G}: \{g \in \mathcal{G} : g \cdot x = x\}$ $\therefore \exists$ bijection between $\mathcal{G}/G_x$ (set of all left cosets of G_x in $\mathcal{G}$), and the orbit $\mathcal{G}x$. The coset aG_x corresponds to element $a \cdot x \in \mathcal{G}x$