10th Lecture: 15/2

Definition 10.1. Let G_1, G_2, $\ldots$, G_n be groups. The *direct product* $G = \prod_{i=1}^n G_i$ is the group such that, the underlying set is the Cartesian product of the G_i and the group operation is defined componentwise, i.e.:

$$(g_1,\, g_2,\, \ldots,\, g_n)(h_1\, h_2,\, \ldots,\, h_n) = (g_1h_1,\, g_2h_2,\, \ldots,\, g_nh_n).$$

In the case of abelian G_i it is common to employ additive notation and write $G = \oplus_{i=1}^n G_i$ and

$$(g_1,\, g_2,\, \ldots,\, g_n) \oplus (h_1\, h_2,\, \ldots,\, h_n) = (g_1 + h_1,\, g_2 + h_2,\, \ldots,\, g_n + h_n).$$

Note that a direct product of groups is abelian if and only if *every* factor is so.

Definition 10.2. Let G and H be groups. A function $\phi : G \to H$ is called a *(group) homomorphism* if

$$\phi(g_1g_2) = \phi(g_1)\,\phi(g_2) \;\; \forall\, g_1,\, g_2 \in G.$$

If, moreover, ϕ is a bijective function then it is said to be a *(group) isomorphism*. We write $G \cong H$ if there exists an isomorphism $\phi : G \to H$ and say that G and H are *isomorphic*. Clearly, isomorphism is an equivalence relation on groups. Isomorphic groups are considered “the same”, from the point of view of abstract algebra.

Example 10.3. In the notation of Exercise 6, Demo3.pdf, let H_9 be the subgroup of D_4 generated by a 180-degree rotation and a reflection in the vertical bisector. Then $H_9 = < a > \times < b >$ is the direct product of two cyclic groups of size 2, generated by the rotation and the reflection separately. Moreover, $H_9 \cong K$, where K is the group of symmetries of a non-square rectangle, the so-called *Klein-4 group*. For one has $K = < c > \times < d >$, where c and d represent reflection in the vertical and horizontal bisectors respectively.

One can make definitions analogous to 10.1 and 10.2 for rings.

Definition 10.4. Let R_1, R_2, $\ldots$, R_n be rings. The *direct product* $R = \prod_{i=1}^n R_i$ is the ring such that, the underlying set is the Cartesian product of the R_i and the ring operations are defined componentwise, i.e.:

$$(r_1,\, r_2,\, \ldots,\, r_n) + (s_1\, s_2,\, \ldots,\, s_n) = (r_1 + s_1,\, r_2 + s_2,\, \ldots,\, r_n + s_n),$$
$$(r_1,\, r_2,\, \ldots,\, r_n) \cdot (s_1\, s_2,\, \ldots,\, s_n) = (r_1 \cdot s_1,\, r_2 \cdot s_2,\, \ldots,\, r_n \cdot s_n).$$

Note that a direct product of rings is commutative (resp. has a unity) if and only if *every* factor is so (resp. has one). In the latter case, the unity in the direct product is $(1,\, 1,\, \ldots,\, 1)$.

Definition 10.5. Let R and S be rings. A function $\phi : R \to S$ is called a *(ring) homomorphism* if

$$\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2), \;\; \phi(r_1r_2) = \phi(r_1)\,\phi(r_2), \;\; \forall\, r_1,\, r_2 \in R.$$

If, moreover, ϕ is a bijective function then it is said to be a *(ring) isomorphism*. We write $R \cong S$ if there exists an isomorphism $\phi : R \to S$ and say that R and S are *isomorphic*. Clearly, isomorphism is an equivalence relation on rings. Isomorphic rings are considered "the same", from the point of view of abstract algebra.

We need one further concept before turning to modular arithmetic.

Definition 10.6. Let R be a ring with unity. The *unit group* $R^\times$ of R is the set of invertible elements in R with the ring multiplication as the group operation, i.e.:

$$R^\times = \{a \in R : \exists\, b \in R \text{ with } ab = ba = 1\}.$$

Note that $R^\times$ is indeed a group since
(i) It is closed under multiplication: $(xy)^{-1} = y^{-1}x^{-1}$
(ii) It contains the identity: $1 \cdot 1 = 1$
(iii) It contains inverses: $(x^{-1})^{-1} = x$.

Examples 10.7. (i) $\mathbb{Z}^\times = \{1\}$ is the trivial ring.
(ii) For any division ring D, $D^\times = D\backslash\{0\}$. In particular, this is true of any field, so in particular of $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.
(iii) If $R = \mathbb{M}_n(\mathbb{R})$, then $R^\times = \mathrm{GL}_n(\mathbb{R})$. One can replace $\mathbb{R}$ by $\mathbb{Q}$ or $\mathbb{C}$, more generally by any field.
(iv) If $R = \prod_{i=1}^n R_i$ is a direct product of rings, then as groups

$$R^\times = \prod_{i=1}^n R_i^\times. \tag{10.1}$$

This is easy to see: an element $(r_1, \ldots, r_n) \in R$ is invertible if and only if each component is so and $(r_1, \ldots, r_n)^{-1} = (r_1^{-1}, \ldots, r_n^{-1})$.

Modular Arithmetic. Let $n \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$. We adopt the standard notation

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \,|\, a - b,$$

and say that a *is congruent to* b *modulo* n.

It is easy to see that, for any fixed $n \in \mathbb{Z}_+$, congruence modulo n is an equivalence relation on $\mathbb{Z}$:
Reflexivity: $a \equiv a \Leftrightarrow n \,|\, a - a \Leftrightarrow n \,|\, 0$, which is obviously true
Symmetry: $a \equiv b \Leftrightarrow n \,|\, a - b \Leftrightarrow n \,|\, b - a \Leftrightarrow b \equiv a$
Transitivity: $(a \equiv b) \wedge (b \equiv c) \Rightarrow (n \,|\, a - b) \wedge (n \,|\, b - c) \Rightarrow n \,|\, (a - b) + (b - c) \Rightarrow n \,|\, a - c \Rightarrow a \equiv c$.

There are n equivalence classes, corresponding to the n possible remainders $0, 1, \ldots, n-1$ upon division by n. The set of equivalence classes is denoted $\mathbb{Z}_n$. It is common to write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, i.e.: to be a bit sloppy and not distinguish between a number and the equivalence class it represents.

The next result yields the fundamental *algebraic* properties of the set $\mathbb{Z}_n$:

Proposition 10.8. *Let $n \in \mathbb{Z}_+$ and let $a, b, c, d \in \mathbb{Z}$ satisfy $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.*

PROOF:

$$a \equiv b \,(\text{mod}\, n) \;\Rightarrow\; n \,|\, a - b,$$
$$c \equiv d \,(\text{mod}\, n) \;\Rightarrow\; n \,|\, c - d.$$

Then, on the one hand,

$$n \,|\, (a - b) + (c - d) \;\Rightarrow\; n \,|\, (a + c) - (b + d) \;\Rightarrow\; a + c \equiv b + d \,(\text{mod}\, n), \text{ v.s.v.}$$

and, on the other hand,

$$[n \,|\, c(a-b)] \wedge [n \,|\, b(c-d)] \;\Rightarrow\; n \,|\, c(a-b) + b(c-d) \;\Rightarrow\; n \,|\, ac - bd \;\Rightarrow\; ac \equiv bd \,(\text{mod}\, n), \text{ v.s.v.}$$

The Proposition implies that addition and multiplication of congruence classes mod n are well-defined, hence that $(\mathbb{Z}_n, +, \cdot)$ is a ring for any $n \in \mathbb{Z}_+$. These are the simplest examples of *finite* rings, since $|\mathbb{Z}_n| = n$ as noted previously. Obviously the ring $\mathbb{Z}_n$ is commutative (since ordinary multiplication of numbers is so) and contains a unity, namely (the class of) 1. We now note two further basic properties:

Proposition 10.9. *The abelian group $(\mathbb{Z}_n, +)$ is cyclic and is generated by an element $a \pmod{n}$ if and only if GCD$(a, n) = 1$.*

PROOF: Let $a \in \mathbb{Z}$. Then a (mod n) generates all of $\mathbb{Z}_n$ under addition if and only if there is no positive integer $k < n$ such that $ka \equiv 0$ (mod n). But $ka \equiv 0 \;\Leftrightarrow\; n \,|\, ka$. From FTA it follows that the smallest positive integer k satisfying this is $k = n/d$, where $d = \text{GCD}(a, n)$. The Proposition follows.

Notation 10.10. In group theory, $\mathbb{Z}_n$ is often used to denote a generic cyclic group of size n. Hence, when seeing this notation, one must always decide from the context wheher it refers to a generic cyclic group of size n or to the specific group of congruence classes modulo n under addition. An alternative notation for the generic cyclic group is C_n.

Proposition 10.11.

$$\mathbb{Z}_n^{\times} = \{a \,(\textit{mod}\, n) : \textit{GCD}(a, n) = 1\}.$$

In particular, $\mathbb{Z}_n$ is a field if and only if n is prime. PROOF: a is invertible mod n if and only if there exists an integer x such that $ax \equiv 1$ (mod n). Now,

$$ax \equiv 1 \,(\text{mod}\, n) \;\Leftrightarrow\; n \,|\, ax - 1 \;\Leftrightarrow\; \exists\, y \in \mathbb{Z} : \, ax - 1 = ny.$$

To summarise, a is invertible mod n if and only if there exist integers x, y satisfying $ax - ny = 1$. But by Bezout's Lemma (Proposition 7.8), such x and y exist if and only if GCD$(a, n) = 1$, v.s.v.

Remark 10.12. The proof of Proposition 10.11 tells us how to actually find multipliciative inverses in $\mathbb{Z}_n$, namely via Euclid's algorithm. I did examples in class, but will do another one in Demo4, so look there instead.

We now have everything in place to prove our two main results, the *Chinese Remainder Theorem* and the *Euler/Fermat theorem*. We do so in the next lecture.