STRUCTURE THEOREM FOR ABELIAN GROUPS. FIELD EXTENSIONS.

R. VIRK

1. Structure theorem for abelian groups

1.1. **Theorem.** *Let G be a finitely generated abelian group. Then*

$$G \simeq \mathbf{Z}^{\oplus n} \oplus \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_m\mathbf{Z},$$

for some integers $m \geq 0$, $d_1, \ldots, d_m > 1$, with $d_1|d_2, d_2|d_3, \ldots, d_{m-1}|d_m$.

Proof. A finitely generated abelian group G is tautologically a finitely generated $\mathbf{Z}$-module. Further, $\mathbf{Z}$ is Noetherian. Hence, G is finitely presented. Let $\mathbf{Z}^{\oplus r} \xrightarrow{f} \mathbf{Z}^{\oplus s} \to G \to 0$ be a presentation of G. We dont distinguish between f and the matrix representing f (with respect to the usual basis for free modules). Write T for the Smith normal form of f. Then T also gives a presentation of G (multiplying by invertible matrices on the left/right of T corresponds to changing bases for $\mathbf{Z}^{\oplus r}$, $\mathbf{Z}^{\oplus s}$). Without loss of generality, we may assume that all the diagonal entries of T are positive and none of them is equal to 1. Let n be the number of zeroes on the diagonal and let $d_1, \ldots, d_m$ be the non-zero entries on the diagonal with $d_1|d_2, \ldots, d_{m-1}|d_m$. Then a moment's thought shows that

$$G \simeq \mathbf{Z}^{\oplus n} \oplus \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_m\mathbf{Z}.$$ □

1.2. **Corollary.** *Let G be a finitely generated abelian group. Then*

$$G \simeq \mathbf{Z}^{\oplus n} \oplus \mathbf{Z}/p_1^{n_1}\mathbf{Z} \oplus \mathbf{Z}/p_2^{n_2}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p_m^{n_m},$$

for some integer $n \geq 0$, prime numbers $p_1, \ldots, p_m$ and integers $n_1, \ldots, n_m \geq 1$.

Proof. Exercise! □

This finishes the 'official' modules part of this course. Once we have covered the other 'official' topics we may (depending on everyone's interest levels) come back to modules.

2. Field extensions

2.1. Let F be a field. An *extension field* (or *field extension*) of F is a field containing F as a subfield.

2.2. *Example.* $\mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. A subfield of $\mathbf{C}$ is also called a *number field.*

2.3. Let $K \supset F$ be a field extension of F. Let $\alpha \in K$. Then α is *algebraic over F* if it is the root of some non-zero monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad \text{with } a_i \in F.$$

The element α is *transcendental over F* if it is not algebraic over F. Note that the notions of algebraic and transcendental depend on the given field F.

2.4. *Example.* $\pi \in \mathbf{R}$ is transcendental over $\mathbf{Q}$.

2.5. *Example.* $\sqrt{-1} \in \mathbf{C}$ is algebraic over $\mathbf{Q}$.

The two possibilities for α can be described in terms of the ring homomorphism

$$\varphi\colon F[x] \to K, \quad f(x) \mapsto f(\alpha).$$

The element α is transcendental over F if and only if φ is injective and algebraic otherwise. Assume α is algebraic. Since $F[x]$ is a PID, $\ker(\phi)$ is generated by a single polynomial $f(x) \in F[x]$ which may as well be assumed to be monic. It is the monic polynomial of lowest degree having α as a root. It is easy to see (exercise!) that $f(x)$ is irreducible. The polynomial f is called the *irreducible polynomial for α over F*. Note that the notion of irreducibility depends on the field F.

2.6. Let $\alpha_1, \dots, \alpha_n \in K$. Denote by $F(\alpha_1, \dots, \alpha_n)$ the smallest subfield of K containing F and $\alpha_1, \dots, \alpha_n$. Denote by $F[\alpha_1, \dots, \alpha_n]$ the *sub-ring* of K generated by F, $\alpha_1, \dots, \alpha_n$. So $F(\alpha_1, \dots, \alpha_n)$ is the fraction field of $F[\alpha_1, \dots, \alpha_n]$.

2.7. **Proposition.** *Let $K \supset F$ be a field extension, $\alpha \in K$. Define a ring homomorphism $\psi\colon F[x] \to F[\alpha], f(x) \mapsto f(\alpha)$.*

(i) *If α is transcendental, then ψ is an isomorphism.*
(ii) *If α is algebraic, with $f(x) \in F[x]$ its irreducible polynomial over F, then ψ induces an isomorphism $F[x]/f(x) \xrightarrow{\sim} F[\alpha]$ and $F[\alpha] = F(\alpha)$. In particular, $F[\alpha]$ is a field.*

Proof. (i) is obvious. In (ii), by definition, $f(x)$ generates the kernel of ψ. The assertion $F[\alpha] = F(\alpha)$ follows from the fact that $f(x)$ is irreducible and hence generates a maximal ideal in $F[x]$. □

2.8. **Proposition.** *Let $K \supset F$ be a field extension. Let $\alpha \in K$ be algebraic over F with irreducible polynomial $f(x)$. Suppose $f(x)$ has degree n. Then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $F[\alpha]$ as a F-vector space.*

Proof. Certainly $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a generating set for $F[\alpha]$ over F (all higher powers of α can be expressed using the given powers using $f(\alpha) = 0$). It must be linearly independent since any relation amongst these elements would give a polynomial $g(x) \in F[x]$ of degree strictly lower than n and such that $g(\alpha) = 0$. □

2.9. A field extension $K \supset F$ is called a *simple extension* if $K = F(\alpha)$ for some $\alpha \in K$, K is called an *algebraic extension* if α is algebraic over F, it is called a *transcendental extension* otherwise.

2.10. **Warning.** An extension may be simple without appearing to be. Take $F = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt{-1}, \sqrt{5})$. Then it is not hard to show that $K = \mathbf{Q}(\sqrt{-1} + \sqrt{5})$.

2.11. Let $K \supset F$ and $K' \supset F$ be field extensions. We say that an isomorphism $f\colon K \xrightarrow{\sim} K'$ is an *F-isomorphism* if f restricts to the identity on the subfield F.

2.12. **Proposition.** *Let $F(\alpha)$ and $F(\beta)$ be simple extensions of F. Assume that α, β are algebraic over F and that they both have the same irreducible polynomial over F. Then $F(\alpha)$ is F-isomorphic to $F(\beta)$.*

Proof. Under the assumptions both $F(\alpha)$ and $F(\beta)$ are F-isomorphic to $F[x]/f$ where f is the common irreducible polynomial of α, β over F. □

2.13. **Warning.** The converse to the above result is false. For instance, $\mathbf{Q}[x]/(x^2-2)$ and $\mathbf{Q}[x]/(x^2 - 4x + 2)$ are $\mathbf{Q}$-isomorphic.

Department of Mathematics, University of California, Davis, CA 95616
E-mail address: virk@math.ucdavis.edu