Corpos Finitos

Vamos a seguir fazer o estudo dos corpos finitos. Embora esses objetos seja bastante abstratos pode-se ver muito da riqueza da Teoria de Galois através deles. Vamos iniciar reunindo algumas informação sobre grupos que usaremos. Acho que todos os textos da bibliografia contem o material que vamos listar sobre grupos.

1 Breve resumo sobre grupos

Iniciamos recordando a definição de grupos.

Definição. Seja G um conjunto com uma operação binária $G \times G \to G$, $(x, y) \in G \times G \longmapsto xy \in G$ que tem as seguintes propriedades:

(i) existe $1 \in G$ tal que $1x = x1 = x$, para todo $x \in G$;

(ii) quaisquer que sejam x, y, $z \in G$ temos $x(yz) = (xy)z$;

(iii) qualquer que seja $x \in G$ existe $x^{-1} \in G$ tal que $xx^{-1} = x^{-1}x = 1$.

Observação. O item (i) acima garante em que G não é vazio. O elemento 1 de que fala o axioma chama-se *elemento neutro* da operação e podemos provar que é único. Muitas vezes é denotado por e.

O axioma (ii) diz que a operação é associativa.

O elemento x^{-1} do axioma (iii) é chamado de *inverso* de x e também é único.

Nos axiomas (i) e (iii) foram escritas as igualdades dos dois lados porque a operação de um grupo não é em geral comutativa.

Caso a operação seja comutativa, dizemos que o grupo é *comutativo* ou *abeliano*.

Quando um grupo G não é abeliano vamos denotar o elemento neutro por 1 e usamos notação multiplicativa para a operação de G. Se G é abeliano denotamos o elemento neutro por 0 e usamos notação aditiva para a operação de G

Acho que os grupos mais conhecidos são os grupos *Simétricos.* Seja S_n o conjunto de todas as bijeções de um conjunto X com n elementos nele mesmo. Mais precisamente, seja $X = \{ 1, 2, \ldots, n \}$

e seja $S_n = \{\, \sigma : X \to X \mid \sigma \text{ é bijetiva } \}$ com a operação de composição de funções. Sabemos que S_n é um grupo que tem $n!$ elementos e é chamado de grupo *Simétrico*. Em S_n o 1 corresponde a função identidade de X.

Temos grupos que são finitos, como no caso acima que S_n tem $n!$ elementos, e temos grupos que são infinitos, como no caso $\mathbb{Z}$ com a operação de adição e neste caso o elemento neutro é o 0.

Outro exemplo importante é o conjunto $\mathrm{GL}_n(K)$ = conjunto das matrizes $n \times n$ que tem determinante $\neq 0$, ou equivalentemente, conjunto das matrizes $n \times n$ que tem inversa. A operação aqui é o produto de matrizes e o 1 é a matriz identidade. Como multiplicar matrizes é associativo, e cada matriz de $\mathrm{GL}_n(K)$ tem uma matriz inversa, por definição de $\mathrm{GL}_n(K)$, esse conjunto é um grupo.

No caso finito definimos:

Definição. Se um grupo G é finito, chama-se *ordem* de G ao número de elementos do conjunto G. **Notação:** $|G|$ = ordem de G.

Da mesmo forma que temos subanel e subcorpo (ou subespaço veotrial) temos também subgrupo.

Definição. Dado um grupo G um subconjunto de $H \subset G$ é chamado de subgrupo se: (i) $1 \in H$, (ii) $\forall\, x,\, y \in H$ resulta $xy \in H$, e (iii) $\forall\, x \in H$ resulta $x^{-1} \in H$. Isto é, H tem o elemento neutro e é fechado para a operação de G e fechado para inversos ($x \in H$ se e só se $x^{-1} \in H$).

Observe que um grupo infinito como $\mathbb{C}^\times$ (com operação dada pela multiplicação) pode conter subgrupos finitos. Por exemplo, se $\xi = \cos(2\pi/n) + \mathrm{sen}\,(2\pi/n)\sqrt{-1}$ é uma raiz primitiva n-ésima da unidade, temos que $< \xi >= \{\, 1, \xi, \ldots, \xi^{n-1}\}$ é um sugbrupo finito de $\mathbb{C}^\times$. Esse grupo é chamado de *cíclico* porque é *gerado* por um único elemento, todos os elementos de $< \xi >$ são "potência" de ξ. Também $\mathbb{Z}$ é cíclico, pois todos os seus elementos são "múltiplos" de 1. Vamos tornar isso mais preciso.

Definição. Dado um grupo G seja $g \in G$.

(i) Para toda todo $s \in \mathbb{Z}$ definimos

$$g^s = \begin{cases} \underbrace{g \cdot g \cdots g}_{s \text{ vezes}} & \text{se } s \geq 1; \\ 1 = \text{elemento neutro} & \text{se } s = 0; \\ \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{|s| \text{ vezes}} & \text{se } s < 0 \end{cases}$$

Caso G seja comutativo trocamos a multiplicação pela soma, assim, para $s \geq 1$ escrevemos $sg = g + g + \cdots + g$, s vezes, para $s = 0$ escrevemos $sg = 0$, etc.

(ii) Seja $< g >= \{ g^n \mid n \in \mathbb{Z} \}$ que chamamos de sugbrupo *gerado* por g. No caso abelianos $< g >= \{ ng \mid n \in \mathbb{Z} \}$.

(iii) Dizemos que G é *cíclico* se existir $g \in G$ tal que $G =< g >$.

Observação. Um fato que convém destacar é que um grupo cíclico tem, em geral, mais de um gerador. O grupo $\mathbb{Z}$ (em relação a adição) tem 1 e -1 como geradores. Para cada n, $\mathbb{Z}/n\mathbb{Z}$ tem, em geral, vários geradores. De fato, $\overline{1}$ é um gerador natural de $\mathbb{Z}/n\mathbb{Z}$; para cada $0 \leq m < n$ podemos escrever $\overline{m} = m\overline{1}$. Por outro lado para cada $1 \leq r < n$ que seja relativamente primo com n temos que $\overline{r}$ é um gerador de $\mathbb{Z}/n\mathbb{Z}$. Como r e n são relativamente primos, sabemos que existem t, $s \in \mathbb{Z}$ tais que $1 = tp + sr$. Portanto $\overline{1} = \overline{sr} = s\overline{r}$. Dessa forma $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >\subset< \overline{r} >\subset \mathbb{Z}/n\mathbb{Z}$, implicando que $< \overline{r} >= \mathbb{Z}/n\mathbb{Z}$.

Apenas no caso $\mathbb{Z}/2\mathbb{Z} = \{ \overline{0}, \overline{1} \}$ temo que $\overline{1}$ é o único gerador do grupo.

Definição. Seja G um grupo e $g \in G$. Se $g \neq 1$, chamamos de *ordem* de g ao mínimo$\{ n \geq 1 \mid g^n = 1\}$. Definimos também que a ordem de 1 é 1 (Atenção: cada um do "1" tem um significado diferente).

Notação: $|g|$ = ordem de g. No caso abelianos temos $|g|$ = mínimo $\{ n \geq 1 \mid ng = 0\}$ e $|0| = 1$.

A ordem de um elemento é bastante especial.

- Dado um grupo G, para todo $g \in G$ temos que $|g|$ divide todo $t \in \mathbb{Z}$ tal que $g^t = 1$ (ou $tg = 0$, no caso abeliano).

Verificando: Se $g = 1$, então $|g| = 1$ e não há nada para demonstrar. Tomemos $g \neq 1$, e seja $t \in \mathbb{Z}$ tal que $g^t = 1$. Pelo Algorítimo de Euclides (em $\mathbb{Z}$) podemos escrever $t = |g|q + r$, com $r = 0$ ou $0 < r < |g|$. Como $r = t - |g|q$ vamos ter $g^r = g^{t-|\varphi|q} = g^t(g^{|g|})^{-q} = 1$, pois $g^t = 1$ e também $g^{|g|} = 1$. Logo $g^r = 1$. Pela minimalidade de $|g|$ vemos temos que $r = 0$ e assim $|g|$ divide t, como queríamos.

Seja $g \in G$ um elemento com ordem finita.

- Como consequência vemos que o conjunto $\{\, g^t \mid t \in \mathbb{Z}\}$, tem que ser finito com exatamente $|g|$ elementos. Na verdade $\{g^t \mid t \in \mathbb{Z}\} = \{1 = g^0,\, g = g^1,\, g^2, \ldots, g^{|g|-1}\,\}$.

Observação. $< g >$ é claramente o menor subgrupo de G contendo g.

Vamos a seguir discutir um resultado que é muito usado em matemática e é conhecido como Teorema de Lagrange.

Seja G um grupo finito e $H \subset G$ um subgrupo. Vamos definir uma relação entre os elementos de G da seguinte maneira:

$$x \equiv y (\mathrm{mod} H) \Leftrightarrow x^{-1}y \in H.$$

Questão 1. Mostre que a relação acima é uma relação de equivalência, isto é, que é reflexiva, simétrica, e transitiva.

Para cada $x \in G$ definimos $\overline{x}$ = classe de equivalência a qual x pertence. Isto é

$$\overline{x} = \{y \in G \mid y \equiv x\,\}.$$

- Temos que $\overline{x} = \{xh \mid h \in H\,\}$. (†)

Temos que mostrar a igualdade de dois conjuntos. Vejamos primeiro que $\overline{x} \subset \{\, xh \mid h \in H\,\}$. Seja $y \in \overline{x} = \{y \in G \mid y \equiv x\,\}$. Logo $h = x^{-1}y \in H$, pela própria definição de $\equiv$. Logo $y = xh \in \{\, xh \mid h \in G\,\}$, demonstrando a primeira inclusão. Vejamos agora que $\{\, xh \mid h \in G\,\} \subset \overline{x}$. Seja $y = xh$, para algum $h \in H$. Então $x^{-1}y = h \in H$. Pela definição de $\equiv$ teremos $x \equiv y$ e assim $y \in \{y \in G \mid y \equiv x\,\}$, que é a outra inclusão. Logo vale a igualdade entre esse conjuntos.

Devido a igualdade acima costuma-se também representar $\overline{x} = xH$ e esse conjunto é chamado de uma *classe lateral a direita* de G módulo H.

Questão 2. Defina uma nova relação de equivalência $\equiv_1$ trocando a ordem de x e y na definição que demos acima de $\equiv$ (isto é troque $x^{-1}y \in H$ por $xy^{-1} \in H$) e mostre que obtemos também uma nova relação de equivalência.

Defina agora $\widehat{x}$ = classe de equivalência dada por $\equiv_1$ a qual x pertence, e mostre que $\widehat{x} = \{\, hx \mid h \in H \,\}$.

Para $\equiv_1$ do exercício acima a notação será mudada para $\widehat{x} = Hx$ e é chamada de *classe lateral a esquerda* de G módulo H.

- Para todo $x \in G$ a classe lateral a direita $\overline{x}$ tem $|H|$ elementos.

Estamos dizendo que todas as classes tem o mesmo número de elementos e que esse número é igual a ordem de H, $|H|$. De fato, considere a função $f : H \to \overline{x} = xH$ dada por $f(h) = xh \in \overline{x}$. Pela propriedade (†) que mostramos acima, f é uma função sobrejetora. Verifiquemos que é injetora: se $f(h_1) = f(h_2)$, então $xh_1 = xh_2$. "Multiplicando-se" essa igualdade pela esquerda por x^{-1} vamos obter $h_1 = h_2$, e assim f é injetora. Portanto f é bijetora e os dois conjuntos tem o mesmo número de elementos, conforme afirmado.

Questão 3. Mostre a mesma coisa para as classes laterais a esquerda, isto é, mostre que $\widehat{x}$ tem $|H|$ elementos, para todo $x \in G$.

Recordemos agora que uma relação de equivalência particiona o conjunto sobre o qual está definida. No nosso caso isso significa que dados x, $y \in G$ temos duas possibilidades excludentes: $\overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \emptyset$.

Esse fato, das duas possibilidades excludentes, é facilmente verificado no nosso caso. Realmente, se existe $z \in \overline{x} \cap \overline{y}$, então $z \equiv x$ e $z \equiv y$. Pela transitividade $x \equiv y$ e portanto $\overline{x} = \overline{y}$.

Talvez fosse bom ressaltamos que $y \in \overline{x}$ se e somente se $\overline{y} = \overline{x}$.

Observemos em seguida que como G é finito, também o conjunto de classes laterais a direita de G módulo H será finito. **Vamos denotar** por G/H ao conjunto de todas as classes laterais a direita de G módulo H. Temos então que $G/H = \{\, \overline{x} \mid x \in G \,\}$. Ao número de elementos de G/H (= número de classe laterais de G módulo H) vamos chamar de *índice* de H em G. **Notação:** $(G : H)$ representa o índice de H em G.

Finalmente, note que como todo $x \in G$ está em alguma classe (na sua própria classe) temos que $G = \bigcup_{x \in G} \overline{x}$. Juntando tudo chegamos a conclusão

Teorema[Lagrange] $|G| = \sum_{x \in G} |\overline{x}| = (G : H)|H|$, onde $|\overline{x}|$ indica o número de elementos do conjunto $\overline{x}$ que sabemos ser igual a $|H|$.

Corolário 1: Seja G um grupo finito e H um subgrupo de G. Então $|H|$ divide $|G|$.

Questão 4. Repita as discussões das últimas 15 linhas para classes laterais a esquerda de G módulo H. Em particular mostre o Teorema de Lagrange trabalhando com $\widehat{x}$ no lugar de $\overline{x}$. Conclua disso que o número de classe laterais a direita, de G módulo H, é igual ao número de classes laterais a esquerda, de G módulo H. Portanto o índice $(G : H)$ não depende de escolhermos uma relação ou a outra.

Corolário 2: Seja G um grupo e $g \in G$. Então $|g|$ divide $|G|$.

De fato, basta lembrarmos que $|g| = | < g > |$.

Outro ponto básico na teoria de grupos é o estudo de homomorfismos.

Definição. Sejam G e S dois grupos e $\varphi : G \to S$ uma função. Dizemos que φ é um homomorfismo de grupos se $\varphi(gh) = \varphi(g)\varphi(h)$ para todo para g, $h \in G$.

Para os homomorfismos de grupos temos propriedades bem semelhantes ao caso de anéis. A composição de dois homomorfismos é um homomorfismo. Analogamente temos epimorfismos e monomorfismos nos casos em que o homomorfismo é sobrejetivo e injetivo. Temos também isomorfismo no caso bijetivo.

Aqui também temos o núcleo.

Definição. Chamamos de núcleo do homomorfismo de grupos $\varphi : G \to S$ ao conjunto $N(\varphi) = \{\, g \in G \mid \varphi(g) = 1 \,\}$.

Temos para o núcleo propriedades análogas àquelas do ideais. Os itens (1) e (3) do resultado abaixo são simples verificação. Quanto ao item (2) basta aplicarmos o Teorema de Lagrange.

Teorema: Seja $\varphi : G \to S$ um homomorfismo de grupos. Então

1. $N(\varphi)$ é um subgrupo de G tal que $gN(\varphi)g^{-1} = N(\varphi)$ para todo $g \in G$. Por outro lado $\mathrm{Im}\,(\varphi) = \varphi(G)$ é um subgrupo de S, chamado de *imagem* de φ.

2. Se G é finito, então $|G| = |N(\varphi)||\mathrm{Im}\,(\varphi)|$. Portanto $|\mathrm{Im}\,(\varphi)|$ divide $|S|$ e $|G|$.

3. φ é injetiva se e somente se $N(\varphi) = \{\,1\,\}$.

Questão 5. Sejam φ e θ dois homomorfismos sobrejetivos de grupo que tem um grupo G como domínio e os grupos S e T como contra-domínios. Mostre que existe um único homomorfismo $\psi : S \to T$ tal que $\psi \circ \varphi = \theta$ se e somente se o núcleo de $N(\varphi) \subset N(\theta)$.

Para provar a existência de ψ no caso $N(\varphi) \subset N(\theta)$, basta definir ψ da maneira obvia: $\psi(\varphi(g)) = \theta(g)$, mostrar que ψ é uma função e que é homomorfismo. Na outra direção é simples verificação.

Os subgrupos com a propriedade (1) do teorema acima são chamados de *normais*.

Definição. Seja G um grupo e H um subgrupo de G. Dizemos que H é um subgrupo *normal* de G se $gHg^{-1} = H$, para todo $g \in G$.

Notação: $H \lhd G$.

A importância dos subgrupos normais vem do fato de que se $H \lhd G$, então as duas relações de equivalência $\equiv$ e $\equiv_1$ definidas na página 4 coincidem e assim toda classe lateral a direita é igual a alguma outra classe lateral a esquerda, isto é, para todo $g \in G$, existe $g' \in G$ tal que $gH = Hg'$. Como consequência se definirmos em $G/H \times G/H \to G/H$ a aplicação $(g_1H, g_2H) \mapsto (g_1g_2H)$ teremos uma função que torna G/H um grupo. Esse grupo é chamado de grupo quociente. Temos também que $\pi : G \to G/H$ dada por $\pi(g) = gH = \overline{g}$ é um homomorfismo sobrejetivo de grupos que tem H como núcleo. Esse homomorfismo π é chamado de *projeção canônica*.

Para os grupos temos também um teorema do isomorfismo cuja demonstração é igual ao caso de anéis.

Teorema do Isomorfismo: $\varphi : G \to S$ um homomorfismo de grupos. Então existe um único homomorfismo de grupos $\overline{\varphi} : G/H \to S$ tal que $\overline{\varphi} \circ \pi = \varphi$, onde $\pi : G \to G/H$ é a projeção canônica.

Mais ainda $\mathrm{Im}\,(\overline{\varphi}) = \mathrm{Im}\,(\varphi)$ e $\overline{\varphi}$ é injetiva.

Como aplicação do teorema acima vamos classificar os grupos cíclicos, pois eles são muito particulares. De fato, se G é um grupo cíclico e g é um gerador de G, $G =< g >$, temos naturalmente uma função $\varphi : \mathbb{Z} \to G$ dada por $\varphi(n) = g^n$ para todo $n \in \mathbb{Z}$.

Questão 6. Verifique que a função φ definida acima é um homomorfismo sobrejetivo de grupos. Caso G seja finito de ordem n, então φ tem núcleo $n\mathbb{Z}$ (agora estamos vendo $\mathbb{Z}$ como grupo aditivo e $n\mathbb{Z}$ como um subgrupo). Usando o Teorema do Isomorfismo conclua que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Caso G não seja finito, mostre que φ é um isomorfismo.

Podemos chegar então a seguinte conclusão: *dois grupos cíclicos finitos de mesma ordem são isomorfos e todo grupo cíclico infinito é isomorfo a* $\mathbb{Z}$. Podemos mesmo dizer que para cada n, $\mathbb{Z}/n\mathbb{Z}$ é o único, a menos de isomorfismo, grupo cíclico de ordem n. Também $\mathbb{Z}$ é, a menos de isomorfismo, o único grupo cíclico infinito.

Questão 7. Uma outra propriedade que mostra como os grupos cíclicos são particulares é que todo subgrupo de um cíclico também é cíclico. De fato, dado um subgrupo H de um grupo cíclico G, escreva $G =< g >$, através de um gerador e tome $r =$ mínimo $\{t \in \mathbb{Z}, t > 0 \mid g^t \in H\}$ Verifique que $H =< g^r >$.

Questão 8. Fugindo um pouco a sequência mostre que se G e S são dois grupos, então $G \times S = \{(g, s) \mid g \in G, s \in S\}$ com a operação $(g, s)(g', s') = (gg', ss')$ é também um grupo.

Estendo o resultado acima considerando um conjunto finito $G_1, G_2, \ldots, G_t$ de grupos e mostre que $G_1 \times G_2 \times \cdots \times G_t$ é um grupo, com a operação definida termo a termo como no caso $n = 2$.

Mostre também que caso $G_1, G_2, \ldots, G_t$ seja grupos finitos, então a ordem de $|G_1 \times G_2 \times \cdots \times G_t| = |G_1|\,|G_2| \cdots |G_t|$.

Vamos a seguir fazer outra aplicação do Teorema do Isomorfismo. Sejam m, n dois inteiros positivos primos entre si. Considere a função $\theta : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ definida por $\theta(s) = (s + m\mathbb{Z}, s + n\mathbb{Z})$.

Questão 9. Mostre que θ é um homomorfismo sobrejetivo de grupos cujo núcleo é $m\mathbb{Z} \cap n\mathbb{Z}$. Para mostrar a sobrejetividade lembre que existe u, $v \in \mathbb{Z}$ tais que $1 = um + vn$. Por causa disso, dados a, $b \in \mathbb{Z}$ tomando-se $c = vna + umb$ vamos ter que $c - a = (vn - 1)a + umb \in m\mathbb{Z}$ e igualmente $c - b \in n\mathbb{Z}$.

Mostre em seguida que $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$ (lembre que m e n são relativamente primos). Podemos então concluir que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}$.

Generalize em seguida, usando indução, esse resultado para um número finito de inteiros positivos $m_1, m_2, \cdots, m_t$, dois a dois primos entre si, mostrando que

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \mathbb{Z}/n_t\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z},$$

onde $n = n_1 n_2 \cdots n_t$ (Compare os fatos acima com o item (d), página 10, da Questão 8 nas Notas IV.).

Voltando aos subgrupos normais temos que outro ponto vantajoso sobre eles é que podemos combiná-los com outros subgrupos.

Definição. Sejam S e T dois subgrupos de um grupo G e assumimos que $S \lhd G$. Então $ST = \{ st \mid s \in S,\ t \in T \}$ também é um subgrupo de G.

Caso $S \cap T = \{ 1 \}$, então cada elemento de ST tem uma única representação na forma st, com $s \in S$, e $t \in T$ e dizemos que ST é um *produto semi-direto* de S e T.

Notação: $S \rtimes T$.

As duas afirmações acima são de fácil verificação, assim como o seguinte resultado:

Teorema: Sejam S e T dois subgrupos de de um grupo G com $S \lhd G$. Então $S \cap T \lhd T$ e $ST/S \simeq T/(S \cap T)$.

A demonstração desse resultado depende somente de observarmos que dados $s \in S$, e $t \in T$ a aplicação $(st)S \mapsto t(S \cap T)$ é o isomorfismo do teorema. Esse resultado é conhecido como *Segundo Teorema do Isomorfismo*

Questão 10. Sejam S, T dois subgrupos normais de um grupo G tais que $S \cap T = \{ 1 \}$. Mostre que $ST \simeq S \times T$.

Caso tomemos um grupo abeliano G vamos observar que a condição de normalidade trivializa-se, isto é, todo subgrupo é normal. Logo, dados quaisquer S, T subgrupos de um grupo abeliano, podemos sempre construir o grupo $S + T = \{ s + t \mid s \in S, t \in T \}$. Caso $S \cap T = \{ 0 \}$ dizemos que temos *soma direta* e denotamos isso por $S \oplus T$.

Podemos também estender essa construção a um número finito de subgrupos. Ficando só no caso abeliano se $S_1, \ldots, S_t$ são subgrupos de G construímos $S_1 + S_2 + \cdots + S_t = \{ s_1 + s_2 + \cdots + s_t \mid s_i \in S_i \}$. Para termos "soma direta" precisamos de um pouco mais de cuidado, temos que exigir que $S_i \cap (S_1 + \cdots + S_{i-1} + S_{i+1} + \cdots + S_t) = \{ 0 \}$, para todo $i = 1, \ldots, t$. Nesse caso escrevemos $S_1 \oplus S_2 \oplus \cdots \oplus S_t$ para indicar esse fato (compare tudo isso com o caso de subespaços de um espaço vetorial).

Mostre que nas condições acima $S_1 \oplus S_2 \oplus \cdots \oplus S_t \simeq S_1 \times S_2 \times \cdots \times S_t$.

Temos também para grupos um Teorema da Correspondência, como no exercício (14) da Questão (9) da página 12, nas Notas IV.

Teorema da Correspondência: Sejam G e S dois grupos e φ um homomorfismo sobrejetivo de G sobre S.

1. Mostre que existe uma correspondência biunívoca entre o conjunto dos sugrupos de G que contém $N(\varphi)$ e o conjunto de todos os subgrupos de S. (Aqui também usamos que se T é um subgrupo de S, então $\varphi^{-1}(T)$ é um subgrupo de G. Mais ainda, se $T \lhd S$, então $\varphi^{-1}(T) \lhd G$).

2. Explore essa correspodência verificando coisas como: ela preserva inclusões, preserva interseções, preserva normalidade, preserva o índice, etc. (Aqui também usamos que se T é um subgrupo de S, então $\varphi^{-1}(T)$ é um subgrupo de G. Mais ainda, $(G : \varphi^{-1}(T)) = (S : T)$, e se $T \lhd S$, então $\varphi^{-1}(T) \lhd G$).

3. Seja H um subgrupo normal de G que contém $N(\varphi)$ e $T = \varphi(H)$. Mostre que $G/H \simeq S/T$. (Use a Questão (5), página 6 para obter um homomorfismo $\psi : G/H \to S/T$ e depois verifique que é um isomorfismo.)

Vamos terminar este resumos com um resultado sobre grupos abelianos que nos será muito útil no estudo dos corpos finitos.

Teorema da Decomposição Canônica Seja G um grupo abeliano finito de ordem n. Seja $n = p_1^{n_1} \cdots p_t^{n_t}$ a fatoração de n em irredutíveis de $\mathbb{Z}$. Para cada $1 \leq i \leq t$ seja

$$G(p_i) = \{ g \in G \mid |g| = p_i^r \text{ para algum } r \geq 0 \}.$$

Temos então que

1. $G(p)$ é um subgrupo de G, para todo p.

2. Se $p_1 \neq p_2$, então $G(p_1) \cap G(p_2) = \{ 0 \}$.

3. Para todo $1 \leq i \leq t$, $|G(p_i)|$ é uma potência de p_i.

4. Para todo $g \in G$ existem e são únicos $g_i \in G(p_i)$ tais que $g = g_1 \cdots g_t$, isto é, $G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_t)$ e assim $G \simeq G(p_1) \times G(p_2) \times \cdots \times G(p_t)$.

   Juntando as conclusões dos itens (3) com (4) podemos concluir que $|G(p_i)| = p_i^{n_i}$ (estamos usando que $\mathbb{Z}$ é um anel fatorial e a Questão 8 da página 8).

Verificação. A demonstração dos dois primeiros itens é simples verificação.

(3). Uma questão que ainda não respondemos é se para todo irredutível p que divide $|G|$ existe $g \in G$ tal que $|g| = p$. Isto é, se as componentes $G(p_i)$ são triviais ou não. Vemos demonstrar abaixo que a resposta a essa pergunta é não, não são triviais, e com isso demonstramos também o fato de que cada $G(p_i)$ tem ordem uma potência de p_i.

Lema: [Cauchy] Seja G um grupo abeliano finito e p um irredutível de $\mathbb{Z}$ que divide $|G|$. Então existe $g \in G$ com $|g| = p$.

Verificação. Se $|G| = p$, pelo que vimos na Questão 6, página 8, $G \simeq \mathbb{Z}/p\mathbb{Z}$. Logo G tem elemento de ordem p. Suponhamos agora que $|G| > p$ e vamos proceder por indução sobre $|G|$.

Seja $u \in G$ com $u \neq 0$. Se $|u| = pm$ para algum $m \in \mathbb{Z}$, então $g = mu$ tem ordem p. Suponhamos que $|u| = n$ e $p \nmid n$.

Como G é abelianos $< u > \lhd G$. Tomemos o grupo quociente $G/ < u >$ que tem ordem $|G|/n$ (lembrar que $| < u > | = |u|$). Temos agora que p divide $|G/ < u > |$, pois p e n são relativamente primos. Temos também que $|G/ < u > | < |G|$. Logo, pela hipótese de indução $G/ < u >$ tem elemento de ordem p. Isto é, existe $h \in G$ tal que $|h+ < u > | = p$. Como $|h|h = 0$ temos que $|h|(h+ < u >) = 0$ $(= 0+ < u >)$ em $G/ < u >$. Novamente pela observação feita no fim da página 3 temos que $p \mid |h|$. Logo $|h| = pm$, como no início da demonstração, e assim $g = mh$ tem ordem p, como queríamos demonstrar.

Voltando então ao Teorema da Decomposição Canônica, o lema acima nos diz que $G(p_i) \neq \{0\}$, para todo $i = 1, \ldots, t$ e como todos os elementos de $G(p_i)$ tem ordem potência de p_i, necessariamente $|G(p_i)|$ é uma potência de p_i.

Para mostrar o item (4) usamos uma forma generalizada do Teorema de Bezout: Para cada $1 \leq i \leq t$ seja $a_i = \prod_{j \neq i} p_j^{n_j}$. Observe que $n = p_i^{n_i} a_i$ e que os números $a_1, \ldots, a_t$ não tem fator comum diferente de ± 1. São em conjunto relativamente primos. Por isso existem inteiros $m_1, \ldots, m_t$

tais que $1 = m_1a_1 + \cdots + m_ta_t$ (Observe que o ideal $I = a_1\mathbb{Z} + \cdots + a_t\mathbb{Z}$, sendo principal, tem a forma $I = u\mathbb{Z}$ para algum $u \in \mathbb{Z}$. Como $a_i \in I$, para todo $i = 1, \ldots, t$ teremos que $u \mid a_i$, para todo i. Logo $u = \pm 1$ e assim $I = \mathbb{Z}$.) Dado $g \in G$, temos que $g = g^1 = g^{m_1a_1}g^{m_2a_2} \cdots g^{m_ta_t}$. Basta agora verificamos que $g_i = g^{m_ia_i} \in G(p_i)$, para todo $i = 1, \ldots, t$.

Isso mostra a existência da decomposição. Para vermos que vale a unicidade temos que verificar se vale a condição da página 9:

$$G(p_i) \cap (G(p_1) + \cdots + G(p_{i-1}) + G(p_{i+1}) + \cdots + G(p_t)) = \{\, 0 \,\}, \quad \text{para todo } i = 1, \ldots, t. \qquad (1)$$

Para fazer a verificação desse fato vamos em primeiro lugar verificar que dados g, $h \in G$, grupo abeliano, se $|g| = a$ e $|h| = b$, então $c(g + h) = 0$, onde c é um mínimo múltiplo comum de a e b. Essa afirmação é claramente correta pois $c = au$ e $c = bv$ para u, $v \in \mathbb{Z}$. Logo $c(g + h) = cg + ch = u(ag) + v(bh) = 0$.

Pergunta: Qual é a condição para que $|g + h| = c$? Sugestão: estude $< g > \cap < h >$.

Mais geralmente dados $g_1, \ldots, g_m \in G$ tais que $|g_i| = a_i$ seja c o mínimo múltiplo comum de $a_1, \ldots, a_m$. Então $c(g_1 + \cdots + g_m) = 0$.

Vamos agora usar essa observação na verificação de que vale a equação (1). Sejam $g_j \in G(p_j)$ para $j = 1, \ldots, t$ tais que $g_i = g_1 + \cdots g_{i-1} + g_{i+1} + \cdots g_t$.

Seja c o mínimo múltiplo comum de $|g_1|, \ldots |g_{i-1}|, |g_{i+1}|, \ldots, |g_t|$. Então c é um produto de potências de $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_t$. Pelo que vimos acima $c(g_1 + \cdots g_{i-1} + g_{i+1} + \cdots g_t) = 0$. Logo $cg_i = 0$, também. Dessa maneira, pela observação feita no fim da página 3 temos que $|g_i|$ divide c. Mas $|g_i|$ é uma potência de p_i e os irredutíveis $p_1, \ldots, p_t$ são distintos. Portanto a única potência de p_i que pode dividir c é 1. Logo $g_i = 0$, ficando demonstrado que a igualdade (1) vale.

Com isso o teorema fica demonstrado.

Questão 11. Usando a Questão 9, página 8, e a Questão 7, página 7, mostre que um grupo abeliano G é cíclico se e somente se $G(p_i)$ é cíclico para todo $i = 1, \ldots, t$.

2 Corpos de Raízes de um Polinômio não Constante

Antes de inciarmos com corpos finitos vamos apresentar alguns resultados que valem em geral, para todos os corpos.

Observação. A partir de agora vamos usar a notação $(f) = f(x)F[x]$ para o ideal principal de um anel de polinômios. Isso vai deixar a equações mais curtas.

Observe inicialmente que o item (e), página 11, da Questão 12 das Notas IV tem como consequência o seguinte fato:

Proposição: Seja F um corpo e $h(x) \in F[x]$ um polinômio não constante. Então existe uma extensão L de F onde $h(x)$ tem todas as suas raízes.

Portanto, se $n = \mathbf{gr}\, h(x)$, existem $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ tais que $h(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$.

Verificação: Basta aplicarmos o item (e) acima mencionado sucessivamente. Isto é, pelo item (e) que citamos existe extensão L_1 onde $h(x)$ tem uma raiz α_1. Em $L_1[x]$ temos $h(x) = (x - \alpha_1)g_1(x)$, para algum $g_1(x) \in L_1[x]$. Se $\mathbf{gr}\, h(x) > 1$, $g_1(x)$ não é constante. Logo, pelo mesmo item (e), existe uma extensão L_2 de L_1 onde $g_1(x)$ tem uma raiz α_2. Em $L_2[x]$ teremos então a decomposição $h(x) = (x - \alpha_1)(x - \alpha_2)g_2(x)$, para algum $g_2(x) \in L_2[x]$. Podemos repetir novamente o processo. Vamos então repetindo esse processo até encontrarmos um corpo que tem todas as raízes de $h(x)$.

Definição. Seja F um corpo e $h(x) \in F[x]$ um polinômio não constante. Dizemos que uma extensão K de F é um *corpo de decomposição* (também chamado de *corpo de raízes*) de $h(x)$ sobre F, se todas as raízes de $h(x)$ estão em K e todo subcorpo intermediário $F \subset E \subsetneqq K$ não tem essa propriedade.

Reformulando, K é um corpo de raízes de $h(x)$ caso $h(x)$ se decomponha em fatores de grau 1, $h(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$, em $K[x]$, e para todo corpo intermediário $F \subset E \subsetneqq K$, $h(x)$ não tenha uma decomposição desse tipo.

Exemplos: (a) Seja $f = x^2 + 3x - 3 \in \mathbb{Q}[x]$. O corpo de raízes de f sobre $\mathbb{Q}$ é $\mathbb{Q}(\sqrt{21})$.

(b) Para $f = x^3 - 5$ temos que $\mathbb{Q}(\sqrt[3]{5}, \xi)$, onde $\xi = \dfrac{-1 + \sqrt{-3}}{2}$ é uma raiz primitiva cúbica da unidade, é o corpo de raízes de f sobre $\mathbb{Q}$. De fato, as raízes de f são $\sqrt[3]{5}$, $\xi\sqrt[3]{5}$, e $\xi^2\sqrt[3]{5}$ que estão em $\mathbb{Q}(\sqrt[3]{5}, \xi)$. Por outro lado qualquer corpo que contenha as três raízes deverá conter também $\xi = \sqrt[3]{5}/\xi\sqrt[3]{5}$.

(c) Para $f = x^4 - 2$ temos que $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$ é o corpo de raízes de f sobre $\mathbb{Q}$.

(d) Claramente $\mathbb{C}$ é o corpo de raízes de $x^2 + 1$ sobre $\mathbb{R}$.

(e) Verifique como exercício que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ é o corpo de raízes de $x^4 - 10x^2 + 1$ sobre $\mathbb{Q}$.

(f) Agora se tomarmos um polinômio mais complicado como por exemplo $x^3 + 3x + 6$ que sabemos

ser irredutível pelo Critério de Eisenstein, então não temos uma descrição do corpo de raízes sobre $\mathbb{Q}$. Mas ainda, se K for o corpo de raízes desse polinômio sobre $\mathbb{Q}$, não sabemos a primeira vista o valor de $[K:\mathbb{Q}]$ que pode ser 3 ou 6 (porque não pode ser outro número?).

Logo para podermos obter informações sobre o corpo de raízes de um polinômio que não seja simples como nos exemplos (a) a (e) precisamos desenvolver uma teoria que permita fazer os cálculos.

Questão 12. Seja $f \in F[x]$ um polinômio não constante e K um corpo de raízes de f sobre F. Para toda extensão intermediária $F \subset E \subset K$ observe que $f \in E[x]$ e mostre que K é um corpo de raízes de f sobre E.

Corolário da Proposição: Para todo corpo F e todo polinômio não constante $h(x) \in F[x]$, existe um corpo de raízes K de $h(x)$ sobre F. Mais ainda, se $h(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ em $K[x]$, então $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Verificação: Pela Proposição acima existe uma extensão L de F onde $h(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ para $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Seja $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset L$. Então $h(x)$ tem todas as suas raízes em K e claro que se $F \subset E \subsetneqq K$, então alguma $\alpha_i \notin E$.

Vamos a seguir demonstrar que o corpo de raízes de um polinômio é único a menos de isomorfismo. Na verdade vamos demonstrar um pouco mais. Sejam F e F' dois corpos e seja $\varphi : F \to F'$ um isomorfismo de corpos. Recordemos que pelo exercício 3, página 5, da Questão 4 das Notas IV podemos estender φ a um isomorfismo $\varphi : F[x] \to F'[x]$ (vamos usar o mesmo símbolo para a extensão de φ a $F[x]$) pondo simplesmente

$$\varphi(a_o + a_1x + \cdots + a_nx^n) = \varphi(a_o) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Teorema da Unicidade: Sejam $F, F', \varphi,\ F[x]$, e $F'[x]$ como acima. Dado um polinômio não constante $f(x) \in F[x]$ denotemos por $f' = \varphi(f) \in F'[x]$.

1. f é irredutível em $F[x]$ se e somente se f' é irredutível em $F'[x]$.

2. Vamos assumir que f é irredutível e que existem extensões L e L' de F e F', respectivamente, com f tendo uma raiz $\alpha \in L$ e f' tendo uma raiz $\alpha' \in L'$. Então existe uma única extensão φ_1

de φ a $F(\alpha)$ tal que $\varphi_1(\alpha) = \alpha'$. Isto é, existe, e é único, isomorfismo $\varphi_1 : F(\alpha) \to F'(\alpha')$ cuja restrição a F é igual a φ tal que $\varphi_1(\alpha) = \alpha'$.

3. Sejam K e K' corpos de raízes de f e f', respectivamente (f qualquer). Então existe isomorfismo $\widetilde{\varphi} : K \to K'$ cuja restrição a F é igual a φ. Dizemos que $\widetilde{\varphi}$ é uma extensão de φ.

   Mais ainda, caso cada fator irredutível de f tenha as raízes distintas, então existem exatamente $[K : F]$ extensões de φ a K.

Verificação: O item (1) é o exercício 18 (a), página 14, da Questão 9 das Notas IV. No caso presente como φ é isomorfismo podemos aplicar o mesmo exercício em φ^{-1} para obter a equivalência. Além disso a afirmação do item (1) é de fácil verificação.

Já o item (2) é o exercício 18 (d), página 14, da mesma Questão 9 das Notas IV. Ou então fazemos diretamente: seja $\pi : F[x] \to F(\alpha)$ o homomorfismo dado por $\pi(h(x)) = h(\alpha)$. Sabemos que π é sobrejetivo e $N(\pi) = (f)$. Correspondentemente seja $\pi' : F'[x] \to F'(\alpha')$ o homomorfismo sobrejetivo com $N(\pi') = (f')$. Observe que temos também homomorfismo $\pi' \circ \varphi : F[x] \to F'(\alpha')$ sobrejetivo e com $N(\pi' \circ \varphi) = (f)$. Definimos então, como no exercício 4, página 5, da Questão 4 das Notas IV, $\varphi_1 : F(\alpha) \to F'(\alpha')$ pondo simplesmente $\varphi_1(\pi(h(x))) = \pi' \circ \varphi(h(x))$. Como π e $\pi' \circ \varphi$ têm o mesmo núcleo, φ_1 é uma função. Verifica-se trivialmente que é um homomorfismo.

Observe agora que $\pi(h(x)) = h(\alpha)$ e que $\pi' \circ \varphi(h(x)) = h'(\alpha')$, onde $h' = \varphi(h)$. Dessa forma, em particular $\varphi_1(\alpha) = \varphi_1(\pi(x)) = \pi' \circ \varphi(x) = \alpha'$. Finalmente, como π e $\pi' \circ \varphi$ são sobrejetoras, também φ_1 vai ser sobrejetora. Com isso demonstramos a existência de um isomorfismo φ_1 como descrito no item (2) no teorema.

Observe agora que dois isomorfismos com a mesma restrição φ a F e satisfazendo a condição de levar α em α' serão necessariamente iguais. Com isso fica demonstrada a unicidade e terminamos a verificação desse item.

Finalmente chegamos ao item (3). Provaremos por indução sobre $[K : F]$. Se $[K : F] = 1$, f se decompõe em fatores lineares em $F[x]$. Logo também f' se decompõe em fatores lineares em $F'[x]$ e $K' = F'$. Logo $\widetilde{\varphi} = \varphi$.

Para $[K : F] > 1$, seja α uma raiz de f e $p(x)$ um polinômio minimal de α sobre F. Se $\mathbf{gr}\, p(x) = 1$, isto é, se $\alpha \in F$ e $f = (x - \alpha)g$, então $\alpha' = \varphi(\alpha)$ é uma raiz de f' e $f' = (x - \alpha')g'$. Nesse caso K é também um corpo de raízes de g sobre F e K' é um corpo de raízes de g' sobre F'. Logo podemos trocar f por g sem modificar o problema. Vamos então assumir que $\mathbf{gr}\, p(x) > 1$.

Seja $p' = \varphi(p)$. Se $f = pg$, com $g \in F[x]$ também $f' = p'g'$ em $F'[x]$. Logo p' tem raiz em K', pois f' tem todas as suas raízes em K' e as raízes de p' estão entre as raízes de f'.

Seja α' uma das raízes de p'. Usando o item anterior estendemos φ a um isomorfismo $\varphi_1 : F(\alpha) \to F'(\alpha')$ com $\varphi_1(\alpha) = \alpha'$. Agora $[K : F(\alpha)] < [K : F]$ e K é um corpo de raízes de $f \in F(\alpha)[x]$ sobre $F(\alpha)$ (conforme Questão 12). Igualmente K' é um corpo de raízes de $f' \in F'(\alpha')[x]$ sobre $F'(\alpha')$. Pela hipótese de indução existe extensão $\widetilde{\varphi} : K \to K'$ de φ_1. Claramente $\widetilde{\varphi}$ é uma extensão de φ.

Para vermos a última parte modificamos um pouco o argumento anterior. Seja p um fator irredutível de f em $F[x]$. Como vimos acima podemos supor que $\mathbf{gr}\, p = m > 1$. Seja $p' = \varphi(p) \in F'[x]$.

Como estamos supondo que p tem raízes distintas, também p' tem raízes distintas. Mais precisamente p' tem $m = \mathbf{gr}\, p'$ raízes distintas, $\alpha'_1, \ldots, \alpha'_m$. Fixando-se uma raiz $\alpha \in K$ de p, pelo item (2) anterior, para cada uma das raízes α'_i, $i = 1, \ldots, m$, de p' temos uma única extensão $\varphi_i : F(\alpha) \to F'(\alpha')$ tal que $\varphi_i(\alpha) = \alpha_i$. Como $\alpha'_1, \ldots, \alpha'_m$ são distintas, também $\varphi_1, \ldots, \varphi_m$ são distintos.

Pela primeira parte desta demonstração do item (3), cada uma das φ_i tem pelo menos uma extensão $\widetilde{\varphi}_i : K \to K'$.

Recorde em seguida que K é um corpo de raízes de f sobre $F(\alpha)$ e K' é um corpo de raízes de f' sobre $F'(\alpha')$. Agora porém $[K : F(\alpha)] = [K : F]/m < [K : F]$, logo pela hipótese de indução cada um dos isomorfismos φ_i tem $[K : F(\alpha)]$ extensões a K. Logo o número total de extensões é $m[K : F(\alpha)] = [K : F]$, como afirmado.

Vejamos em seguida que não podemos ter mais do que $[K : F]$ extensões, isto é, vejamos que as extensões encontradas acima representam todas as possíveis extensões.

Seja $\theta : K \to K'$ um isomorfismo tal que $\theta|_F = \varphi$. Mantemos a mesma raiz $\alpha \in K$ de p fixada anteriormente. Temos então que $0 = \theta(p(\alpha)) = p'(\theta(\alpha))$. Portanto $(\theta(\alpha))$ é uma raiz de p' e então existe $1 \leq i \leq m$ tal que $\alpha'_i = \theta(\alpha)$. Vemos também que a restrição de θ a $F(\alpha)$ é um isomorfismo $F(\alpha) \to F(\alpha')$ que estende φ e satisfaz a condição $\theta(\alpha) = \alpha'_i$. Logo, pela unicidade estabelecida no item (2), θ restrito a $F(\alpha)$ é igual a φ_i e assim θ é uma das extensões contadas anteriormente. Conclusão, o número de extensões é $[K : F]$, como queríamos.

Observação. Convém observar que o processo de indução descrito acima, pode ser visto como um algorítimo recursivo para construir todas as extensões de φ a K.

Vejamos qual é a idéia: sejam $\beta_1, \ldots, \beta_m$ as raízes distintas de p. Num primeiro passo construímos

m extensões $\varphi_i : F(\beta_1) \to F'(\alpha_i')$, como descrito acima.

Num segundo passo, seja $q \in F(\beta_1)[x]$ um fator irredutível de p. Como as raízes de q estão entre as raízes de p, temos $q(\beta_t) = 0$, para algum t. Como no argumento anterior vamos supor que $\mathbf{gr}\, q > 1$ e assim $\beta_t \neq \beta_1$. Seja agora $q_i' = \varphi_i(q) \in F(\alpha_i')[x]$, para um $1 \leq i \leq m$. Teremos que q_i' divide p' em $F'(\alpha_i')[x]$ e assim q_i' terá suas raízes entre as raízes $\alpha_1', \ldots, \alpha_m'$ de p'. Observe que como q é irredutível em $F(\beta_1)[x]$, também q_i' é irredutível em $F(\alpha_i')[x]$ e, em particular, $q_i'(\alpha_i') \neq 0$. Seja α_{j_s}' uma raiz de q_i'.

Estendemos em seguida φ_i a um único isomorfismo $\varphi_{i,j_s} : F(\beta_1, \beta_t) \to F(\alpha_i', \alpha_{j_s}')$ com $\varphi_{i,j_s}(\beta_t) = \alpha_{j_s}$, pelo item (2) do teorema.

Como no caso inicial, obtemos uma extensão de φ_i para cada raiz de q_i'. Isto é, φ_i terá $\mathbf{gr}\, q_i'$ extensões desse tipo.

Em seguida vemos que cada φ_i dá origem a um q_i', todos com o mesmo grau, e cada um deles dá origem a $\mathbf{gr}\, q_i'$ extensões de φ_i.

Temos assim um processo que vai "subindo" de F para K contando o número de extensões em cada etapa.

Por exemplo para $K = \mathbb{Q}(\sqrt[3]{5}, \xi)$ como no exemplo (b) de página 13, temos que id tem 3 extensões distintas

$$\varphi_1 = \mathrm{id} : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{Q}(\sqrt[3]{5}),\ \varphi_2 : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{Q}(\xi\sqrt[3]{5}),\ \varphi_3 : \mathbb{Q}(\sqrt[3]{5}) \to \mathbb{Q}(\xi^2\sqrt[3]{5}),$$

uma para cada raiz de $x^3 - 5$. Cada uma delas terá 2 extensões distintas para K. Observe que $K = F(\xi\sqrt[3]{5})$, onde $F = \mathbb{Q}(\sqrt[3]{5})$. Neste caso temos só duas etapas para ir de $\mathbb{Q}$ à K. Sejam então as extensões de φ_1 à K: $\varphi_{1,1} = \mathrm{id}$ e $\varphi_{1,2}$ caracterizada por $\varphi_{1,2}(\xi\sqrt[3]{5}) = \xi^2\sqrt[3]{5}$ (logo $\varphi_{1,2}(\xi) = \xi^2$).

As extensões de φ_2 são: $\varphi_{2,1}(\xi\sqrt[3]{5}) = \xi^2\sqrt[3]{5}$ (logo $\varphi_{2,1}(\xi) = \xi$) e $\varphi_{2,2}(\xi\sqrt[3]{5}) = \sqrt[3]{5}$ (logo $\varphi_{2,2}(\xi) = \xi^{-1} = \xi^2$).

Analogamente construímos as extensões de φ_3 "levando" $\xi\sqrt[3]{5}$ em cada uma das outras duas raízes de $x^3 - 5$.

Questão 13. Faça uma construção semelhante para obter todos os 8 isomorfismos de $\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1}) \to \mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})$ correspondente ao exemplo (c) da página 13.

Corolário: Sejam F um corpo, $f \in F[x]$ não constante, e sejam K e K' dois corpos de raízes de f sobre F. Então exite isomorfismo $\sigma : K \to K'$ que deixa os elementos de F fixos ponto a ponto.

Mais ainda, caso cada fator irredutível de f tenha raízes distintas, então temos $[K : F]$ desses isomorfismos.

Verificação: Basta aplicar o teorema anterior com $\varphi = \text{id}$, onde id é a função identidade de F.

Dizer que σ deixa os elementos de F fixos ponto a ponto é o mesmo que dizer que a restrição de σ a F é igual a id. Observe que podemos ver σ como uma F-transformação linear de K em K'.

Um outro ponto que convém destacar e que caso $f = p_1^{n_1} \cdots p_m^{n_m}$, com $n_i > 0$ para todo $i = 1, \ldots, m$, seja a decomposição de f em fatores irredutíveis de $F[x]$ e tomarmos $g = p_1 \cdots p_m$, então f e g tem o mesmo conjunto de raízes, embora com multiplicidades diferentes, e portanto pelo corolário da página 12 tem mesmo corpo de raízes.

A hipótese de que cada fator irredutível de f tem raízes distintas significa que cada p_i tem raízes distintas.

No teorema acima necessitarmos que cada fator irredutível de $f(x)$ tenha raízes distintas. Polinômios com essa propriedade recebem um nome especial:

Definição. Dizemos que um polinômio $f(x) \in F[x]$ é separável se cada fator irredutível de $f(x)$ tem raízes distintas. Dizemos também que os fatores irredutíveis de $f(x)$ tem raízes simples.

No momento pode não ser claro que um polinômio irredutível possa ter alguma raiz com multiplicidade > 1. Depois do estudo sobre corpos finitos voltaremos a esse ponto.

3 Fecho Algébrico de um Corpo

Vamos agora definir fecho algébrico de um corpo e demonstrar que todo corpo tem um único, a menos de isomorfismo, fecho algébrico. Os argumentos que vamos usar são semelhantes aos usados na seção anterior.

Recordemos que um corpo Ω é chamado de algebricamente fechado se todo polinômio não constante $f \in \Omega[x]$ tem uma raiz em Ω. Logo todos os irredutíveis de $\Omega[x]$ são polinômios de grau 1.

Recordemos também que uma extensão K de um corpo F é chamada de algébrica se todo $\alpha \in K$

for algébrico sobre F, i.e., existe polinômio não constante $f \in F[x]$ tal que $f(\alpha) = 0$.

Definição. Seja F um corpo e Ω uma extensão algébrica de F tal que Ω é algebricamente fechado. Dizemos então que Ω é um *fecho algébrico* de F.

Questão 14. Seja F um corpo e Ω um fecho algébrico de F. Seja $F \subset E \subset \Omega$ uma extensão intermediária. Mostre que Ω também é um fecho algébrico de E.

Teorema: Todo corpo F tem um fecho algébrico.

Verificação Construirmos inicialmente um corpo onde todos os polinômio não constantes de $F[x]$ tenham raiz. Fazemos isso generalizando o processo usado no no item (d) do exercício 12 da página 11 das Notas IV.

Para cada polinômio não constante $f \in F[x]$ vamos definir um símbolo X_f e tomamos $\mathcal{X} = \{\, X_f \mid f \in F[x], \mathbf{gr}\, f \geq 1 \,\}$. Seja agora o anel de polinômio $F[\mathcal{X}]$ constituído de todos os polinômios em variáveis de $\mathcal{X}$. Um elemento típico de $F[\mathcal{X}]$ tem a forma

$$\sum_{f_1,\ldots,f_n \in F[x]} a_{f_1,\ldots,f_n} X_{f_1}^{i_{f_1}} \cdots X_{f_n}^{i_{f_n}},\ a_{f_1,\ldots,f_n} \in F,$$

que não é nada bonita.

Tomemos agora I o ideal de $F[\mathcal{X}]$ gerado por todos os elementos da forma $f(X_f)$, com $f(x) \in F[x]$, não constante. Afirmamos que $I \neq F[\mathcal{X}]$. Suponhamos o contrário, para chegar a um absurdo. Logo existem $f_1, \ldots, f_n \in F[x]$ e $g_1, \ldots, g_n \in F[\mathcal{X}]$ tais que

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1. \qquad (\dagger)$$

Seja agora K um corpo onde $f_1, \ldots, f_n$ tem uma raiz, que vamos chamar de α_i. Observe que basta tomarmos um corpo de raízes de $h = f_1 f_2 \cdots f_n$ para obtermos o corpo K. Para todas as variáveis X_f que aparecerem nos polinômios $g_1, \ldots, g_n$ que forem diferentes de $X_{f_1}, \ldots, X_{f_n}$ tomamos $\alpha_f = 0$. Trocando-se agora todas as variáveis que aparecem na equação (†) pelos correspondentes αs vamos obter $0 = 1$; a contradição procurada. Logo I é um ideal próprio de $F[\mathcal{X}]$ e podemos tomar um ideal maximal $\mathfrak{m}$ de $F[\mathcal{X}]$ contendo I. Seja $E = F[\mathcal{X}]/\mathfrak{m}$, o anel quociente. Como $\mathfrak{m}$ é maximal, E é um corpo. Seja $\pi : F[\mathcal{X}] \to E$ a projeção canônica. Como $I \cap F = \{\, 0 \,\}$ temos que a restrição de π a F é injetiva. Identificando $F = \pi(F)$, podemos considerar E como uma extensão de F. Observe agora que $\pi(f(X_f)) = 0$, para todo $f \in F[x]$, não constante. Logo $\pi(X_f)$ é uma raiz de $f = \pi(f)$ (lembrar

que $F = \pi(F)$). Tomamos agora F_1 o fecho algébrico de F em E como no item (iv) da definição, página 1, das Notas III. Logo todo $f \in F[x]$ não constante tem raiz em F_1, pois tem raiz em E. Mais ainda F_1 é uma extensão algébrica de F.

Em seguida repetimos essa construção com F_1 no lugar de F e obtemos uma extensão F_2 de F_1 tal que todo $g \in F_1[x]$ tem raiz em F_2 e F_2 é uma extensão algébrica de F_1. Por transitividade F_2 também é uma extensão algébrica de F. Vamos repetindo esse processo e obtemos uma cadeia

$$F = F_o \subset F_1 \subset F_2 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots$$

Tomamos agora $\Omega = \bigcup_{j=0}^{\infty} F_j$, que é uma extensão algébrica de F, pois cada F_i é algébrico sobre F.

Vejamos que Ω é algebricamente fechado. De fato, se $g \in \Omega[x]$ é um polinômio não constante, exite $j \geq 0$ tal que $g \in F_j[x]$. Pela construção feita, g tem raiz em $F_{j+1} \subset \Omega$.

A seguir queremos mostrar que o fecho algébrico é único, a menos de isomorfismo. Vamos demonstrar um pouco mais.

Teorema: Seja $\varphi : F_1 \to F_2$ um isomorfismo entre dois corpos F_1 e F_2. Seja Ω_i um fecho algébrico de F_i, para $i = 1, 2$. Então existe um isomorfismo $\widetilde{\varphi} : \Omega_1 \to \Omega_2$ que estende φ.

Verificação Seja $\mathcal{E} = \{ (E, \varphi_E) \}$ tais que $F_1 \subset E \subset \Omega_1$ é uma extensão de F e $\varphi_E : E \to \Omega_2$ é um homomorfismo (injetivo) que estende φ.

Como o par $(F_1, \varphi) \in \mathcal{E}$ temos que $\mathcal{E} \neq \emptyset$. Ordenemos agora $\mathcal{E}$ da seguinte maneira: $(E, \varphi_E) \leq (K, \varphi_K)$ se e somente se $E \subset K$ e a restrição de φ_K a E é igual a φ_E. Verifica-se trivialmente que essa relação é uma relação de ordem parcial em $\mathcal{E}$.

Seja agora $(E_i, \varphi_i) \in \mathcal{E}$, para todo $i \in I$ um subconjunto de $\mathcal{E}$ totalmente ordenado por essa relação. Tomando-se $E_o = \bigcup_{i \in I} E_i$ teremos uma extensão de F contida em Ω_1. Definimos $\varphi_o : E_o \to \Omega_2$ por $\varphi_o(\alpha) = \varphi_i(\alpha)$ se $\alpha \in E_i$. Verifica-se facilmente que φ_o é um homomorfismo e portanto $(E_o, \varphi_o) \in \mathcal{E}$. Como $(E_i, \varphi_i) \leq (E_o, \varphi_o)$, para todo $i \in I$ concluímos que toda cadeia ascendente de elementos de $\mathcal{E}$ tem um extremo superior. Logo, pelo Lema de Zorn, $\mathcal{E}$ contém elementos maximais. Seja $(K, \varphi_K) \in \mathcal{E}$ um elemento maximal. Vamos mostrar que $K = \Omega_1$ e que φ_K tem Ω_2 como imagem.

Vamos denotar por K' a imagem de K por φ_K dentro de Ω_2. Logo $\varphi_K : K \to K'$ é um isomorfismo de corpos. Vemos também que Ω_2 é uma extensão algébrica de K'. Na verdade é um fecho algébrico de K'.

Suponhamos, por absurdo, que existe $\alpha \in \Omega_1$ com $\alpha \notin K$. Como α é algébrico sobre F também é algébrico sobre K. Seja $g(x) \in K[x]$ um polinômio minimal de α e seja $g^{'}$ sua imagem através de φ_K em $K^{'}[x]$. Temos que $g^{'}$ também é irredutível. Tomemos $\alpha^{'}$ uma raiz de $g^{'}$ em Ω_2. Pelo item (2) do Teorema da Unicidade, página 14, φ_K estende-se a um isomorfismo $\varphi_1 : K(\alpha) \to K^{'}(\alpha^{'}) \subset \Omega_2$. Mas então o para $(K(\alpha), \varphi_1)$ está em $\mathcal{E}$ e como $(K, \varphi_K) < (K(\alpha), \varphi_1)$ obtemos uma contradição com a maximalidade de (K, φ_K). Logo $K = \Omega_1$, como queríamos. Vejamos agora que $K^{'} = \operatorname{Im} \varphi_K = \Omega_2$. Novamente supomos que existe $\beta \in \Omega_2$ com $\beta \notin K^{'}$. Seja $h \in K^{'}[x]$ um polinômio minimal de β. Temos que $\mathbf{gr}\, h > 1$, pois $\beta \notin K^{'}$. Com $h(x)$ está na imagem de φ_K existe polinômio $h_o \in \Omega_1[x]$ tal que $\varphi(h_o) = h$ (Estamos usando a notação introduzida na página 14 antes do Teorema da Unicidade.). Como h é irredutível, também h_o é irredutível, item (1) do Teorema de Unicidade. Mas isso é uma contradição com Ω_1 ser algebricamente fechado, pois h_o é irredutível e tem grau > 1. Portanto $K^{'} = \Omega_2$, como queríamos e $\widetilde{\varphi} = \varphi_K$ é o isomorfismo procurado.

Corolário: Sejam Ω_1 e Ω_2 dois fechos algébricos de um corpo F. Então $\Omega_1 \simeq \Omega_2$.

Verificação Basta aplicarmos o teorema acima com $F_1 = F_2 = F$ e $\varphi = \mathrm{id}$.

4 Corpos Finitos

Iniciamos por recordar o exercício 19, página 14, da Questão 9 das Notas IV. Se K é um corpo finito, então $c(K) = p \neq 0$ ($c(K)$ é a característica de K, ver exercício 10, página 2, da Questão 1 das Notas IV) e $[K : \mathbb{F}_p]$ é finito. Logo K tem p^n elementos. Isto é, todo corpo finito tem p^n elementos, onde p é a característica do corpo. Vejamos nosso primeiro resultado.

Proposição: Seja K um corpo finito com p^n elementos.

1. Todo $\alpha \in K$ é raiz do polinômio $x^{p^n} - x \in \mathbb{F}[x]$ e K é o corpo de raízes desse polinômio sobre $\mathbb{F}$.

2. Se $K^{'}$ for outro corpo finito com p^n elementos, então existe um isomorfismo $\theta : K \to K^{'}$ cuja restrição a $\mathbb{F}_p$ é a identidade (Dizemos que θ é um $\mathbb{F}_p$-isomorfismo).

3. O grupo multiplicativo $K^{\times}$ é cíclico com ordem $p^n - 1$. Para $\delta \in K^{\times}$ um gerador desse grupo temos que $K = \mathbb{F}_p(\delta)$.

4. Seja $\varphi : K \to K$ a função dada por $\varphi(\alpha) = \alpha^p$, para todo $\alpha \in K$. Então φ é um $\mathbb{F}_p$-automorfismo de K tal que $\varphi^n = \mathrm{id}$ e para todo $1 \leq r < n$ temos $\varphi^r \neq \mathrm{id}$.

   Na verdade, dado $\alpha \in K$ temos que $\varphi(\alpha) = \alpha$ se e somente se $\alpha \in \mathbb{F}_p$.

Verificação: (1) Seja $\alpha \in K$. Podemos assumir que $\alpha \neq 0$, pois 0 é claramente raiz do polinômio $x^{p^n} - x$. Logo $\alpha \in K^\times$ que é um grupo de ordem $p^n - 1$. Pelo Corolário 2 da página 6, temos que

$$\alpha^{p^n-1} = 1, \quad \text{ou equivalentemente} \quad \alpha^{p^n-1} - 1 = 0.$$

Logo α é raiz do polinômio $x^{p^n} - x$.

Finalmente, como K tem p^n elementos e todos são raízes do polinômio $x^{p^n} - x$ que tem grau p^n, concluímos que K consiste no conjunto de todas as raízes desse polinômio. Logo K só pode ser o corpo de raízes desse polinômio sobre $\mathbb{F}_p$.

(2) Pelo item (1) todo corpo com p^n elementos é o corpo de raízes de $x^{p^n} - x$ sobre $\mathbb{F}_p$. Estamos também assumindo que $\mathbb{F}_p$ está contido em todo corpo de característica p. Basta então aplicarmos o corolário da página anterior para terminarmos a demonstração deste item.

(3) Vamos agora usar que $K^\times$ é um grupo abeliano de ordem $p^n - 1$ Seja $p^n - 1 = p_1^{n_1} \cdots p_t^{n_t}$ a decomposição de $p^n - 1$ em fatores irredutíveis de $\mathbb{Z}$. Pela Questão 11 da página 12 temos que mostrar que cada componente $G(p_i)$ de $K^\times$ é cíclica. Pelo comentário final do Teorema da Decomposição Canônica, página 10, sabemos que $|G(p_i)| = p_i^{n_i}$. Para simplificar a notação vamos escrever simplesmente $G(p)$ com ordem p^r, onde p é qualquer um dos p_i e r o correspondente n_i, e demonstrar que $G(p)$ é cíclico.

Tomemos $\alpha \in G(p)$ de forma que $|\alpha| = p^s$ seja o maior valor assumido pelas ordens dos elementos de $G(p)$. Então se $\beta \in G(p)$ teremos $\beta = p^{s(\beta)}$, para algum $s(\beta) \leq s$. Logo, para todo $\beta \in G(p)$, temos que $|\beta|$ divide p^s. Consequentemente $\beta^s = 1$, para todo $\beta \in G(p)$. Isto é, todo $\beta \in G(p)$ é raiz do polinômio $x^{p^s} - 1$. Resulta disso que $G(p)$ tem no máximo p^s elementos. Como $|G(p)| = p^r$ temos que $r \leq s$

Por outro lado, como $|\alpha| = p^s$, pelo Corolário 2 da página 6, $p^s \mid p^r = |G(p)|$. Logo $s \leq r$. Juntando as duas desigualdades temos $s = r$ e assim $|\alpha| = |G(p)|$. Logo $G(p) =< \alpha >$ é um grupo cíclico. Isto é, cada uma das componentes $G(p_i)$ é cíclica e também $K^\times$ é cíclico.

Seja agora $\delta \in K^\times$ tal que $K^\times =< \delta >$. Claramente $F(\delta) = K$.

(4) Aqui também vamos demonstrar um resultado preparatório.

Lema: Sejam $p \in \mathbb{Z}$ um irredutível e $1 \leq s \leq p-1$. Então o coeficiente binomial $\binom{p}{s} = \dfrac{p!}{s!(p-s)!}$ é divisível por p.

Verificação: Como sabemos que

$$\binom{p}{s} = \frac{p(p-1)\cdots(p-s+1)}{s!},$$

é um número inteiro, necessariamente $s!$ divide o produto $p(p-1)\cdots(p-s+1)$. Mas $s!$ é um produto de números menores do que o primo s. Logo $s!$ e p são relativamente primos em $\mathbb{Z}$. Portanto $s!$ divide $(p-1)\cdots(p-s+1)$ em $\mathbb{Z}$. Assim,

$$\frac{(p-1)\cdots(p-s+1)}{s!} \quad \text{é um número inteiro, e} \quad p\frac{(p-1)\cdots(p-s+1)}{s!} \quad \text{é um múltiplo de } p,$$

conforme afirmado.

Voltemos a demonstração do item (4). Claramente $\varphi(1) = 1$ e $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$, quaisquer que sejam α, $\beta \in K$. Vejamos que $\varphi(\alpha+\beta) = \varphi(\alpha)+\varphi(\beta)$, ou equivalentemente que $(\alpha+\beta)^p = \alpha^p + \beta^p$. Pela fórmula do Binômio de Newton sabemos que

$$(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \binom{p}{2}\alpha^{p-2}\beta^2 + \cdots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p.$$

Pelo lema acima p divide todos os coeficientes $\binom{p}{s}$ para $1 \leq s \leq p-1$. Como K tem característica p isso significa que para todo $1 \leq s \leq p-1$, $\binom{p}{s} = 0$. Logo $(\alpha+\beta)^p = \alpha^p + \beta^p$, como queríamos.

Vemos assim que φ é um homomorfismo de anéis. Como K é um corpo, φ é injetivo. Finalmente, como K é finito a injetividade implica que φ é sobrejetivo. Logo φ é um isomorfismo, como afirmado.

Por outro lado, sabemos que $\mathbb{F}_p \subset K$ é exatamente o conjunto das raízes de $x^p - x$. Portanto, para $\alpha \in K$, temos $\alpha^p = \alpha$ se e somente se $\alpha \in \mathbb{F}_p$. Ou então, $\varphi(\alpha) = \alpha$ se e somento se $\alpha \in \mathbb{F}_p$.

Observe em seguida que $\varphi^j(\alpha) = \alpha^{p^j}$, para todo $j \geq 0$. Pelo item (1) podemos então concluir que $\varphi^n = \mathrm{id}$ e para todo $1 \leq r < n$, $\varphi^r \neq \mathrm{id}$, completando a demonstração do teorema.

Observação. (a) Um isomorfismo $\sigma : K \to K$ de um corpo K nele mesmo é chamado de *automorfismo*. O automorfismo φ do item (4) do teorema acima é chamado de automorfismo de Frobenius.

(b) Dado um corpo K que é uma extensão de um corpo F, um automorfismo de K, $\sigma : K \to K$, cuja restrição a F é a identidade é chamado de *F-automorfismo de K*. O conjunto de todos os F-automorfismo de K é um grupo em relação a composição de funções. Denotaremos esse grupo por $G(K;F)$. Convém observar que $G(K;F)$, em geral, não é abeliano e com frequência é trivial. Por exemplo $G(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q}) = \{\,\mathrm{id}\,\}$. De fato, dado $\sigma \in G(\mathbb{Q}(\sqrt[3]{2});\mathbb{Q})$, temos que $\sigma(\sqrt[3]{2})^3 = \sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$. Portanto $\sigma(\sqrt[3]{2})$ é uma das raízes de $x^3 - x$. Como $\sigma(\sqrt[3]{2}) \in \mathbb{Q}(\sigma(\sqrt[3]{2})) \subset \mathbb{R}$, vemos que $\sigma(\sqrt[3]{2})$ é a única raiz de $x^3 - 2$ em $\mathbb{Q}(\sigma(\sqrt[3]{2}))$. Logo $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. Finalmente como a restrição de σ a $\mathbb{Q}$ é a identidade, vamos obter que $\sigma = \mathrm{id}$.

Definição. Seja K uma extensão algébrica de um corpo F. O grupo $G(K;F)$ é chamado de grupo de Galois da extensão.

Recorde que definimos que um polinômio não constante $f \in F[x]$ como sendo separável se todos os seus fatores irredutíveis em $F[x]$ tiverem raízes simples (Ver página 18, no fim da Seção 3).

Definição. Seja K o corpo de raízes de um polinômio não constante e separável com coeficientes em um corpo F. Nessas condições K é chamado de uma extensão galoisiana de F.

Questão 15. Seja $d \in \mathbb{Z}$ um inteiro livre de quadrados. Mostre que a função $\sigma(a+b\sqrt{d}) = a-b\sqrt{d}$ é um $\mathbb{Q}$-automorfismo de $\mathbb{Q}(\sqrt{d})$. Verifique em seguida que $G(\mathbb{Q}(\sqrt{d});\mathbb{Q}) = \{\,\mathrm{id}, \sigma\,\}$.

Questão 16. Mostre que o único automorfismo de $\mathbb{Q}$ é a identidade. Igualmente o único automorfismo de $\mathbb{F}_p$ é a identidade. Logo, para todo corpo K temos que um automorfismo σ de K restrito ao seu corpo primo é a identidade.

Questão 17. Sejam K uma extensão de um corpo F e $\sigma \in G(K;F)$. Seja também $f(x) \in F[x]$ um polinômio não constante que tem uma raiz $\alpha \in K$. Mostre que $\sigma(\alpha)$ também é uma raiz de $f(x)$.

Questão 18. Dado um polinômio não constante com raízes distintas $f(x) \in F[x]$, seja K um corpo de raízes de $f(x)$ sobre F. Usando o corolário da página 17 mostre que $|G(K;F)| = [K : F]$. Observe que K é uma extensão galoisiana de F.

Questão 19. Seja K uma extensão galoisiana de um corpo F. Conforme a questão anterior $G(K;F)$ tem $[K:F]$ elementos. Definimos agora norma $N : K \to F$ pondo para cada $\alpha \in K$

$$N(\alpha) = \prod_{\sigma \in G(K;F)} \sigma(\alpha) \tag{2}$$

Mostre que $N : K^\times \to F^\times$ é um homomorfismo de grupos. Mostre também que ImN contêm $(F^\times)^{[K:F]}$.

Questão 20. Seja K um corpo finito com p^n elementos. Mostre que $G(K:\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$. Isto é, $G(K:\mathbb{F}_p)$ é cíclico de ordem n (mostre que o automorfismo de Frobenius gera $G(K:\mathbb{F}_p)$).

Questão 21. Determine $G(K;\mathbb{Q})$ onde K é o corpo de raízes dado nos exemplos (a), (b), (c) e (e) da página 13.

Voltaremos aos corpos finitos depois de termos desenvolvido a Teoria de Galois, como o que ficará muito simples continuar o estudo. Antes porém vamos apresentar um resultado com argumentos elementares para mais tarde vermos o quanto ganhamos em usar a Teoria de Galois.

Teorema: Seja K um corpo finito com $c(K) = p$ (característica de K) e $n = [K:\mathbb{F}_p]$. Temos então:

1. Se $\mathbb{F}_p \subset E \subset K$ é um corpo intermediário, então $m = [E:\mathbb{F}_p]$ divide n
2. Para todo divisor positivo m de n existe (e é único) corpo intermediário $\mathbb{F}_p \subset E_m \subset K$ com $m = [E_m:\mathbb{F}_p]$.
3. Sejam m e d dois divisores positivos de n e E_m, E_d respectivamente, os corpos intermediários correspondentes. Então $m \mid d$ se e somente se $E_m \subset E_d$.

Verificação. (1) vale em geral para toda extensão intermediária: $[K:\mathbb{F}_p] = [K:E][E:\mathbb{F}_p]$. Vejamos agora (2). Para isso vamos usar a seguinte identidade polinomial: sejam s e t dois inteiros positivos, então

$$x^{st} - 1 = (x^s - 1)(x^{(s-1)t} + x^{(s-2)t} + \cdots + x^t + 1). \tag{3}$$

Para um divisor positivo m de n temos $n = mt$. Substituindo-se x por p na identidade acima, com $st = n$ e $s = m$, obtemos $p^n - 1 = (p^m - 1)\ell$, onde $\ell = p^{(m-1)t} + p^{(m-2)t} + \cdots + p^t + 1$ é um

inteiro positivo. Usamos novamente a identidade (3) com $st = p^n - 1$ e $s = p^m - 1$ obtemos que

$$x^{p^n-1} - 1 \quad \text{divide} \quad x^{p^m-1} - 1$$

em $\mathbb{F}_p[x]$. Logo todas as raízes de $x^{p^m-1} - 1$ estão entre as raízes de $x^{p^n-1} - 1$. Pelo item (1) da Proposição da página 21, sabemos que $K^\times$ é exatamente o conjunto de todas as raízes de $x^{p^n-1} - 1$. Tiramos desse fato duas informações:

(a) todas as raízes de $x^{p^n-1} - 1$ são distintas. Consequentemente também $x^{p^m-1} - 1$ tem $p^m - 1$ raízes distintas;

(b) Todas as raízes de $x^{p^m-1} - 1$ estão em K.

Seja agora $E = \{$ todas as raízes de $x^{p^m-1} - 1 \} \cup \{ 0 \}$. Vemos que E consiste no conjunto de todos os elementos de K que são raízes da equação $x^{p^m} - x$. Já vimos que dados α, $\beta \in K$ vale $(\alpha + \beta)^p = \alpha^p + \beta^p$. Recursivamente verificamos que também vale $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$. Resulta disso que dados α, $\beta \in E$, teremos $\alpha + \beta \in K$. Por outro lado

$$(\alpha\beta)^{p^m} - \alpha\beta = \alpha^{p^m}\beta^{p^m} - \alpha\beta^{p^m} + \alpha\beta^{p^m} - \alpha\beta = (\alpha^{p^m} - \alpha)\beta^{p^m} + \alpha(\beta^{p^m} - \beta) = 0,$$

e assim $\alpha\beta \in E$. Conclusão E é um subcorpo de K com p^m elementos. Logo $[E : \mathbb{F}_p] = m$, como queríamos.

(3) Se $E_m \subset E_d$, então $d = [E_d : \mathbb{F}_p] = [E_d : E_m][E_m : \mathbb{F}_p]$ e $m \mid d$. Reciprocamente, se $m \mid d$ obtemos como acima que $x^{p^m-1} - 1$ divide $x^{p^d-1} - 1$ e portanto $E_m^\times = \{$ todas as raízes de $x^{p^m-1} - 1 \}$ está contido em $\{$ todas as raízes de $x^{p^d-1} - 1 \} = E_d^\times$. Logo $E_m \subset E_d$, como afirmado.

Em nosso estudo sobre corpo finitos ainda falta demonstrarmos que para todo n existe um corpo com p^n elementos. Ainda não podemos fazer isso porque não podemos garantir que o polinômio $x^{p^n} - x \in \mathbb{F}_p[x]$ sempre tem raízes distintas. Precisamos então estabelecer um critério para verificar que um dado polinômio tem raízes distintas e então demonstrar a existência de corpos com p^n elementos, para todo $n \geq 1$.