Ordes van oplosbare permutatiegroepen

Dit onderwerp sluit aan op het in het najaar in een nationale *master course* gedoceerde vak *Permutatiegroepen*, en is in het bijzonder aantrekkelijk voor studenten die dat vak gevolgd hebben. Onderstaande beschrijving begint met een samenvatting van een aantal dingen die op het genoemde college behandeld zijn.

Voor een positief geheel getal n definiëren we $T(n) = \max\{\#G : G$ is een eindige oplosbare groep waarvoor er een trouwe transitieve G-verzameling X met $\#X = n$ bestaat$\}$. Uit de Galoistheorie volgt dat $T(n)$ de grootste orde is van de Galoisgroep van de normale afsluiting van een separabele lichaamsuitbreiding $K \subset L$ van graad n die oplosbaar is door radicalen. Dit is één van de belangrijkste redenen om in $T(n)$ geïnteresseerd te zijn.

Het blijkt dat $T(n)$ als functie van n tamelijk snel kan groeien, en dat het in vele omstandigheden beter is om een minder snel groeiende functie P te bekijken, die alleen gedefinieerd is op priemmachten $q = p^k$ (met p priem en k een positief geheel getal), als volgt: $P(q) = \max\{\#G : G$ is een eindige oplosbare groep waarvoor er een trouwe primitieve G-verzameling X met $\#X = q$ bestaat$\}$. (Een G-verzameling X heet *primitief* als X transitief is en bovendien het aantal G-invariante equivalentierelaties op X gelijk is aan 2; hierbij noemt men een op X gedefinieerde equivalentierelatie *G-invariant* als voor elk tweetal equivalente elementen x, y van X en elke $\sigma \in G$, de elementen σx en σy eveneens equivalent zijn.) De functie P laat weer een Galoistheoretische beschrijving toe: $P(q)$ is de grootste orde is van de Galoisgroep van de normale afsluiting van een separabele lichaamsuitbreiding $K \subset L$ van graad q die oplosbaar is door radicalen en bovendien de eigenschap heeft dat het aantal tussenlichamen van de uitbreiding $K \subset L$ gelijk is aan 2. (Zo'n uitbreiding bestaat dan en slechts dan als q een priemmacht is.)

Men kan $T(n)$ in $P(q)$ uitdrukken: er geldt dat $T(n)$ het maximum is van alle getallen

$$P(q_1)^{q_2 \cdots q_t} \cdot P(q_2)^{q_3 \cdots q_t} \cdot \ldots \cdot P(q_{t-1})^{q_t} \cdot P(q_t),$$

waarbij $(q_1, q_2, \ldots, q_t)$ loopt over alle rijtjes van niet-negatieve lengte t met de eigenschap dat alle q_i priemmachten zijn en $q_1 q_2 \cdots q_t = n$.

Bij de bestudering van de functie P komt men de functie S tegen, eveneens op priemmachten q gedefinieerd: $S(q) = \max\{\#G : G$ is een eindige oplosbare groep waarvoor er een trouw simpel G-moduul M met $\#M = q$ bestaat$\}$. Het verband tussen S en P wordt gegeven door de eenvoudige formule $P(q) = q \cdot S(q)$. Om, tenslotte, S te bestuderen, definieert men eerst wanneer men een G-moduul *primitief* noemt. Deze definitie lijkt op de bovengegeven definitie van een primitieve G-verzameling, vandaar dat men hetzelfde woord gebruikt. Vervolgens zet men $R(q) = \max\{\#G : G$ is een eindige oplosbare groep waarvoor er een trouw primitief G-moduul M met $\#M = q$ bestaat$\}$. Dan kan men bewijzen dat $S(p^k)$ gelijk is aan het maximum van alle getallen $R(p^d)^e \cdot T(e)$, waarbij d, e over alle paren positieve gehele getallen met $de = k$ loopt.

De functie R is eenvoudig genoeg om in de meeste gevallen rechtstreeks uit te rekenen. Er blijkt dat voor alle $q = p^k$ met slechts eindig veel uitzonderingen geldt: $R(p^k) = k \cdot (p^k - 1)$.

Tot zover het op college behandelde. Het eerste onderwerp van een bachelor-onderzoek kan eruit bestaan om alle getallen p^k te vinden waarvoor $R(p^k)$ *niet* gelijk is aan $k \cdot (p^k - 1)$, en tevens voor deze p^k de juiste waarde van $R(p^k)$ te bepalen. Het is waarschijnlijk dat deze lijst met enig zoeken in de literatuur gevonden kan worden, maar ook dan is het interessant om te zien hoeveel groepentheorie er, na het op college behandelde, nog gaat zitten in het bewijs dat de lijst compleet en correct is.

Een tweede onderwerp gaat ervan uit dat het eerste onderwerp volledig is afgehandeld, zodat de functie R volledig bekend is. Is er een kans dat voor de getallen $T(n)$, $P(q)$ en $S(q)$ een gesloten formule gevonden kan worden, met eventueel een overzichtelijk aantal apart te behandelen uitzonderingen, net als in het geval van $R(q)$? Ook als dit niet zo mocht zijn, kan men zich afvragen hoe men bij gegeven n of q de getallen $T(n)$, $P(q)$ of $S(q)$ zo snel mogelijk uitrekent, waarbij het in het geval van $T(n)$ redelijk is aan te nemen dat de volledige priemfactorizatie van n bekend is.

Bij dit tweede onderwerp komt verder geen groepentheorie kijken. Er is wel nog een aantal andere kwesties van meer algebraïsche aard die aansluiten op het gegeven college en in een bacheloronderzoek uitgediept kunnen worden. Hierover kan men contact opnemen met de begeleider.

Begeleider: H. W. Lenstra.